Lageman, Bernhard; Rothgang, Michael; Friedrich, Werner

Research Report

Durchführung der erweiterten Erfolgskontrolle beim Programm zur Förderung der Industriellen Gemeinschaftsforschung und -entwicklung (IGF) im Zeitraum 2005-2009. Weiterentwicklung des Programms zur Förderung der industriellen Gemeinschaftsforschung: Vorschläge und Begründungen. April 2007

RWI Projektberichte

Provided in Cooperation with:

RWI – Leibniz-Institut für Wirtschaftsforschung, Essen

RWI : Projektberichte

Rheinisch-Westfälisches Institut
für Wirtschaftsforschung und
WSF Wirtschafts- und Sozialforschung

Erweiterte Erfolgskontrolle beim Programm zur Förderung der IGF im Zeitraum 2005–2009

Forschungsvorhaben im Auftrag des
Bundesministeriums für
Wirtschaft und Technologie

Weiterentwicklung des Programms zur
Förderung der industriellen
Gemeinschaftsforschung

RWI
ESSEN

WSF

RWI : Projektberichte

Herausgeber: Rheinisch-Westfälisches Institut für Wirtschaftsforschung,
Hohenzollernstraße 1/3, 45128 Essen
Tel. 0201/81 49-0, Fax 0201/81 49-200, e-mail: rwi@rwi-essen.de

Schriftleitung: Prof. Dr. Christoph M. Schmidt, Ph.D.

Durchführung der erweiterten Erfolgskontrolle beim Programm zur Förderung der Industriellen Gemeinschaftsforschung und -entwicklung (IGF) im Zeitraum 2005–2009
Forschungsvorhaben im Auftrag des
Bundesministeriums für Wirtschaft und Technologie (BMWi)
Weiterentwicklung des Programms zur Förderung der industriellen Gemeinschaftsforschung
April 2007

Rheinisch-Westfälisches Institut
für Wirtschaftsforschung und
WSF Wirtschafts- und Sozialforschung

Durchführung der erweiterten Erfolgskontrolle beim Programm zur Förderung der Industriellen Gemeinschaftsforschung und -entwicklung (IGF) im Zeitraum 2005–2009

Forschungsvorhaben im Auftrag des
Bundesministeriums für Wirtschaft und Technologie
Weiterentwicklung des Programms zur Förderung der
industriellen Gemeinschaftsforschung –
Vorschläge und Begründungen
April 2007

RWI
ESSEN

WSF

Projektteam

RWI Essen
Dr. Bernhard Lageman, Dr. Michael Rothgang

WSF Wirtschafts- und Sozialforschung
Dr. Werner Friedrich

Das Projektteam dankt Verena Eckl, Dr. Jochen Dehio, Wolfgang Dürig, Dr. Dirk Engel, Marlies Tepaß und Dr. Lutz Trettin für die Unterstützung bei der Durchführung des Projekts.

Inhalt

Vorbemerkung

Im Rahmen der Förderung der industriellen Gemeinschaftsforschung (IGF) wurden in den letzten Jahren intensive Anstrengungen unternommen, die Unternehmen, insbesondere KMU, stärker in alle Phasen der Projektanbahnung und -durchführung zu integrieren. Es besteht jedoch kein Zweifel daran, dass nach wie vor eine stärkere Mitwirkung von KMU in der IGF wünschenswert wäre und die Forschungsergebnisse die mittelständische Wirtschaft in höherem Maße erreichen sollten, als dies bislang offensichtlich der Fall ist. In diesem Zusammenhang ist eine Erhöhung des Bekanntheitsgrads des Programms und der Institutionen der Gemeinschaftsforschung dringend erforderlich. Die Arbeitsgemeinschaft industrieller Forschungsvereinigungen „Otto von Guericke“ e.V. (AiF) und die Forschungsvereinigungen (FV), sollten insgesamt wesentlich größere Anstrengungen zur Förderung des Ergebnistransfers unternehmen. Sie sollten hierbei auf in der IGF und in anderen Programmen entwickelte „best practices“ zurückgreifen.

Der vorliegende Beitrag enthält Vorschläge zur Weiterentwicklung der IGF, die sich auf Erfahrungen aus der erweiterten Erfolgskontrolle stützen. Er ist wie folgt gegliedert: Der erste Gliederungspunkt enthält Vorschläge zur Programmrichtlinie, der zweite beschäftigt sich mit dem Ergebnistransfer, der dritte mit den Antrags- und Begutachtungsverfahren, im vierten werden Vorschläge zur Verbesserung des Programmmonitorings aufgelistet und begründet. Die Vorschläge sind jeweils eingangs in den grau unterlegten Feldern dargestellt und über den gesamten Text hinweg durchgehend nummeriert. Den Vorschlägen schließen sich jeweils die mehr oder weniger ausführlich ausfallenden Begründungen an.

1. Programmatik

Das Programm zur Förderung der industriellen Gemeinschaftsforschung wurde zwar bereits in den 1950er Jahren begründet, die hierdurch initiierten Aktivitäten – Entwicklung von Forschungsnetzwerken und Kooperation zwischen Unternehmen und Wissenschaft – muten aus Sicht der heutigen ökonomischen Innovationsforschung trotz des Alters des Programms aber ausgesprochen modern an. Die Programmdokumente haben diese Entwicklung in wesentlichen Punkten nachvollzogen. Dies ist allerdings nicht in allen Aspekten im wünschenswerten Maße geschehen.

Vorschlag 1

Wir schlagen folgende neue Formulierung für die Definition der Aufgaben der IGF in der Richtlinie vor:

1 Zuwendungszweck, Zielgruppe und Rechtsgrundlage

1.1 Die industrielle Gemeinschaftsforschung (IGF) hat das Ziel, durch die Unterstützung vorwettbewerblicher Forschungsprojekte insbesondere kleinen und mittleren Unternehmen den Zugang zu Forschungsergebnissen zu erleichtern. Von der Förderung sollen insbesondere die Unternehmen des innovativen Mittelstands im Verarbeitenden Gewerbe, darunter auch die innovativen Teile des Handwerks sowie Unternehmen des Dienstleistungssektors, für die technisch-ingenieurswissenschaftliche Fragestellungen relevant sind, profitieren.

Die IGF unterstützt die Entwicklung von Forschungsnetzwerken zwischen der mittelständischen Wirtschaft, staatlichen Hochschulen und unabhängigen Forschungsinstituten. Im Rahmen der Arbeitsgemeinschaft industrieller Forschungsvereinigungen „Otto von Guericke" e.V. (AiF) schlagen Forschungsvereinigungen branchenweit bzw. für ein Technologiefeld relevante Forschungsvorhaben vor, die durch Universitätsinstitute oder unabhängige Forschungseinrichtungen (Forschungsstellen) bearbeitet werden sollen. Der Zugang zu den im Rahmen der IGF durchgeführten Aktivitäten steht grundsätzlich für alle interessierten Unternehmen offen.

1.2 Die Verbreitung der Ergebnisse der IGF in der Wirtschaft, insbesondere bei den mittelständischen Unternehmen wird im Rahmen des Programms aktiv gefördert. Die Resultate der IGF-geförderten Vorhaben stehen allen Unternehmen ohne Einschränkung zur Verfügung. Um die Attraktivität des Programms für die mittelständische Wirtschaft zu erhöhen, werden Unter-

nehmen des Mittelstand in die Projektauswahl und -durchführung einbezogen sowie intensive Bemühungen zur Optimierung und Verkürzung der Antragsprozeduren unternommen.

Aufgrund des systemischen Charakters vieler für KMU relevanter technologischer Fragestellungen und der Vernetzung der mittelständischen Wirtschaft mit Großunternehmen in industriellen Wertschöpfungsketten ist es für die Erreichung der Zielsetzung der IGF unabdingbar und liegt im Sinne des Programms, dass auch Großunternehmen in diese Strukturen eingebunden sind.

1.3 Aufbauend auf den Ergebnissen der vorwettbewerblichen IGF-Förderung können mittelständische Unternehmen firmenspezifische Lösungen für neue Verfahren, Produkte und Dienstleistungen entwickeln, um so ihre Wettbewerbsfähigkeit zu verbessern.

Begründung

Gegenüber der bestehenden Programmbegründung sollten einige zentrale Punkte ergänzt bzw. stärker hervorgehoben werden. Das betrifft den Netzwerkcharakter der Förderung. Auch an zentraler Stelle angesprochen werden sollten die Bedeutung des Wissenstransfers, die möglichst frühzeitige und umfassende Einbindung von KMU in die Entscheidungsprozesse sowie die Bemühungen um eine Optimierung der Auswahlprozeduren. Dies sind zentrale Pfeiler der Weiterentwicklung des Programms. Der Ergebnistransfer wird – so unser Eindruck – teilweise noch als „Pflichtprogramm“ betrachtet, das man im Anschluss an das Projekt zu absolvieren hat, dagegen weniger als das, was er eigentlich ist: ein entscheidendes „Nadelöhr“, das letztlich über den langfristigen Programmerfolg entscheidet. Die Veränderung des Bewusstseins beginnt damit, dass man die Bedeutung, die dem Transfer, aber auch den anderen genannten Punkten, in der Programmbegründung und im Rahmen der formulierten Programmziele zukommt, wahrnimmt.

Vorschlag 2

Um einen einheitlichen Auftritt des Programms sicherzustellen, sollte strikt darauf geachtet werden, dass die verschiedenen Programmbeschreibungen (im Leitfaden der AiF, auf den Internetseiten der AiF und des BMWi) vereinheitlicht werden. Die verschiedenen Dokumente sollten sich jeweils an der Programmrichtlinie orientieren.

Begründung

In den verschiedenen relevanten Quellen (Programmrichtlinie, AiF-Leitfaden, Internet-Seiten von AiF und BMWi, Haushaltsplan) finden sich zum Teil unterschiedliche Begründungen der AiF-Förderung, die jeweils unterschiedliche Aspekte des Programms betonen. Ein Blick auf die Zielbeschreibungen des Programms in den verschiedenen Quellen zeigt zumindest eine gewisse Heterogenität. Um dies zu demonstrieren, seien nachstehend einige Zielbeschreibung aufgeführt.

– Unterstützung dauerhafter Forschungskooperationen in branchenweiten Netzwerken (Haushalt);

– Ziel, insbesondere KMU den Zugang zu Forschungsergebnissen zu erleichtern, die sie benötigen, um den Anschluss an den technischen Fortschritt zu halten (Haushalt).

– auf Grundlage der vorwettbewerblichen Ergebnisse der IGF können Unternehmen firmenspezifische Lösungen für neue Verfahren, Produkte und Dienstleistungen entwickeln, um so ihre Wettbewerbsfähigkeit zu verbessern (Haushalt);

– Durchführung branchenweiter, vorwettbewerblicher Gemeinschaftsforschungsprojekte von Forschungsvereinigungen vorwiegend kleiner und mittlerer Unternehmen im Rahmen der AiF (Internetseite des BMWi);

– Ausgleich von strukturbedingten Nachteilen von KMU auf dem Gebiet der FuE (Internetseite der AiF);

- KMU können ihre gemeinsamen Probleme durch gemeinsame Forschungsaktivitäten lösen, die vor allem durch Hochschulen und gemeinnützige wirtschaftsnahe Forschungseinrichtungen durchgeführt werden (Internetseite der AiF);

– die industrielle Gemeinschaftsforschung soll Orientierungswissen erarbeiten und technologische Plattformen für ganze Branchen oder zur branchenübergreifenden Nutzung entwickeln (Richtlinie);

– dauerhafte Forschungskooperationen in branchenweiten und/oder übergreifenden Netzwerken unterstützen (Richtlinie);

– KMU den Zugang zu praxisnahen Forschungsergebnissen ermöglichen; dabei entspricht ein Zusammenwirken von KMU und großen Unternehmen den Grundsätzen der industriellen Gemeinschaftsforschung und -entwicklung (Richtlinie);

– FuE-Aktivitäten, die von einer repräsentativen Mehrheit kleinerer und mittlerer Unternehmen einer industriellen Wirtschaftsbranche oder eines industriellen Technologiefeldes im Rahmen einer entsprechenden Mitgliedsvereinigung gemeinsam und folglich vorwettbewerblich betrieben werden (Leitfaden);

– mittelständische Unternehmen können Nutzen aus den für die Unternehmen gleichermaßen zugänglichen Forschungsergebnissen ziehen und dadurch ihre strukturbedingten Nachteile auf dem Gebiet der FuE teilweise ausgleichen (Leitfaden).

Die hier aufgeführten Zielsetzungen sind weitgehend miteinander kompatibel und betonen jeweils einzelne Aspekte des Programms. Eine stärkere Fokussierung auf ein zentrales Ziel und die klare Unterscheidung von Basisziel und abgeleiteten – instrumentalen – Zielen wäre allerdings zweckdienlich.

2. Ergebnistransfer

Zu den grundlegenden Zielsetzungen des Programms gehört die breite Streuung der durch gemeinschaftliche Forschung gewonnenen Erkenntnisse unter den kleinen und mittleren Unternehmen. Das Wissen um die Forschungsergebnisse erweitert die Optionen der Unternehmen für technische Lösungen, die wiederum einen Beitrag zur Verbesserung ihrer Wettbewerbsfähigkeit leisten können. Eine solche Zielsetzung ist zwangsläufig mit der Anforderung verbunden, das Wissen über eine Vielzahl von Kanälen zu verbreiten und möglichen Anwendern nahe zu bringen. Der Transfer der Forschungsergebnisse zu den Unternehmen ist daher eine zentrale Voraussetzung für den Erfolg und die Wirksamkeit des Programms. Hier besteht offenkundig noch ein erheblicher Handlungsbedarf, wobei insbesondere den Forschungsvereinigungen für die Weiterentwicklung der Transferprozesse eine tragende Rolle zukommt. Die Verbesserung des Transfers ist für den Erfolg des Programms unabdingbar.

Vorschlag 3

Der Abschnitt 2 „Gegenstand der Förderung“ in der Richtlinie sollte einen Abschnitt enthalten, der die Verpflichtung zur Durchführung der im Projektantrag genannten Transfermaßnahmen festschreibt.

2.6 Für die Erstzuwendungsempfänger (Forschungsvereinigungen) besteht im Rahmen der öffentlich geförderten Forschungsvorhaben die Verpflichtung,

*während der Durchführung des Projekts und nach dessen Abschluss die im Antrag genannten Transfermaßnahmen durchzuführen. Die Forschungsstellen unterstützen die **jeweiligen** Forschungsvereinigungen bei Durchführung der Transfermaßnahmen.*

Begründung

Der Technologietransfer „lebt" von der aktiven Bemühung um die wirtschaftliche Ergebnisverwertung. Um zu verhindern, dass das Projekt nach der Lösung des technischen Problems „abgehakt" wird, muss tatsächlich sichergestellt sein, dass die erforderlichen Maßnahmen ergriffen werden. Unser Vorschlag steht in unmittelbarem Zusammenhang mit den Vorschlägen zur Veränderung von Abschnitt 3.6 im Leitfaden der AiF und zu den Vorschlägen zur Anpassung der Gliederung für den Projektantrag und im Gutachterfragebogen (siehe unten).

Vorschlag 4

Klare Zuordnung der Verantwortung für die Durchführung der Transfermaßnahmen in Zusammenarbeit mit den Forschungsstellen an die Forschungsvereinigungen. Diese Zuordnung sollte sich in der Richtlinie niederschlagen: Formulierungsvorschlag für Punkt 2.3 der Richtlinie:

Die Anträge zu den FuE-Vorhaben müssen entsprechende Transfervorschläge, Aussagen zur Umsetzbarkeit und zur wirtschaftlichen Bedeutung einschließen. Die Forschungsstellen unterstützen die Forschungsvereinigungen aktiv bei den erforderlichen Transfermaßnahmen und führen neben den Forschungsvereinigungen im Rahmen ihrer Möglichkeiten eigene Transfermaßnahmen im Anschluss an die Projekte durch.

Begründung

Bei einem (eher kleineren) Teil der IGF-Projekte sind Unternehmen, die direkt an der Übernahme und Weiterentwicklung der IGF-Ergebnisse interessiert sind, von vornherein in den PA einbezogen. In einem solchen Kontext ist der Ergebnistransfer zumindest in die partizipierenden Unternehmen hinein auf eine elegante Art „vorprogrammiert". Auch in diesen Fällen stellt sich allerdings die Frage, wie das gewonnene Wissen an solche Unternehmen weiter vermittelt werden kann, die nicht am Projekt beteiligt sind, aber sehr wohl am Forschungsthema interessiert sein müssten.

In den weitaus meisten Fällen ist der Weg von der Durchführung der Projekte bis zu jenem Punkt, an dem Unternehmen auf für sie relevante Aspekte der Forschung aufmerksam werden, sehr weit. Erfolgreicher Technologietransfer erfordert systematische Anstrengungen, die über die Bekanntmachung der Ergebnisse weit hinausgehen. Die bisherigen Formulierungen im Leitfaden zur Veröffentlichung der Forschungsergebnisse (Abschnitt 3.6) erscheinen hier zu weich und passiv. Sie leisten der Schwierigkeit der Aufgabe des Technologietransfers zu wenig Rechnung. Die aktive Verantwortung für und die Durchführung von Maßnahmen durch die Forschungsvereinigungen sollte daher an zentraler Stelle in der Richtlinie verankert sein.

Vorschlag 5

Der Abschnitt 3.6 „Veröffentlichung der Forschungsergebnisse" im Leitfaden sollte neu formuliert werden und die Erfordernisse des Technologietransfers enthalten. Unser Formulierungsvorschlag lautet:

3.6 *Transfer und Publikation der Forschungsergebnisse*

3.6.1 Ergebnistransfer

Für die Erstzuwendungsempfänger im Rahmen der öffentlich geförderten Forschungsvorhaben besteht gemäß der Förderrichtlinie die Verpflichtung, während des Projekts und im Anschluss an dieses die im Antrag genannten Transfermaßnahmen durchzuführen. Die Forschungsvereinigungen werden bei den Transfermaßnahmen von den jeweiligen Forschungsstellen unterstützt.

3.6.2 Verpflichtung zur Veröffentlichung der Ergebnisse

Der Erstzuwendungsempfänger ist verpflichtet, die Forschungsergebnisse innerhalb von sechs Monaten nach Ende des Bewilligungszeitraums in geeigneter Form zu veröffentlichen. Ein Exemplar dieser Veröffentlichung ist der AiF-Hauptgeschäftsstelle sofort nach Drucklegung vorzulegen und als pdf-Datei zur Verfügung zu stellen.

Darüber hinaus sind die Ergebnisse der öffentlich geförderten Forschungsvorhaben für die interessierte Öffentlichkeit und die Adressaten der Förderung in deutscher Sprache zu veröffentlichen. In jeder Veröffentlichung ist darauf hinzuweisen, dass das Forschungsvorhaben (mit IGF-Nr. und Buchstabe nach Zuwendungsbescheid) aus Haushaltsmitteln des Bundesministeriums für Wirtschaft und Technologie (BMWi) über die Arbeitsgemeinschaft industrieller Forschungsvereinigungen(AiF) gefördert worden ist.

Unbenommen der Veröffentlichung in schriftlicher Form ist die zuständige Forschungsvereinigung verpflichtet, eine zeitnahe Veröffentlichung der Ergebnisse des Forschungsprojekts und einer Kurzdarstellung (innerhalb von sechs Monaten nach Abschluss) als pdf-Datei im Internet vorzunehmen.

3.6.3 Erfüllung der Verpflichtung zum Ergebnistransfer

Die Veröffentlichung der Forschungsergebnisse ist ein wichtiger Aspekt des Ergebnistransfers, jedoch in vielen Fällen nicht ausreichend. Es muss vielmehr sichergestellt werden, dass die Adressaten des Projekts in einer geeigneten Weise über dessen Projekte und Inhalte informiert werden. Je nach Forschungsprojekt können dabei unterschiedliche Maßnahmen geeignet sein. Die Veröffentlichung in einer Fachzeitschrift oder als Dissertation wird allerdings vornehmlich die Adressaten im wissenschaftlichen Bereich, häufig dagegen nicht in Unternehmen, zumal in KMU, erreichen. Daher ist zu überprüfen, inwieweit andere Formen der Verbreitung (Vorträge vor Verbandsgremien, Messepräsentationen usw.) besser geeignet für den Ergebnistransfer sind.

Die Überprüfung der Frage, welche Transfermaßnahmen ausreichend sind, ist Gegenstand des Antragsverfahrens. Die tatsächliche Durchführung der Transfermaßnahmen ist mit adäquatem Abstand zum Abschluss der Projekte, spätestens aber ein Jahr nach dem formellen Projektabschluss, einer formellen Prüfung zu unterziehen. Hierzu erstatten die Forschungsvereinigungen in standardisierter Form Bericht an die AiF. Die AiF sammelt die Berichte und berichtet ihrerseits in strukturierter und komprimierter Form über die Transfermaßnahmen in einem Transferbericht an das BMWi.

Falls sich im Projektverlauf erforderliche Anpassungen in den Transferplanungen ergeben, sind diese zu begründen und zum Projektabschluss der zuständigen Forschungsstelle mitzuteilen.

Begründung

Der Leitfaden und die zugrunde liegenden Regelungen zur Veröffentlichung der Ergebnisse sollten stärker als bisher die Erfordernisse der Transferprozesse widerspiegeln. Die Veröffentlichung der Forschungsergebnisse im Anschluss an das Projekt als Projektbericht lässt sich zwar leicht kontrollieren, jedoch ist sie – je nach Projekt – häufig nicht ausreichend, um sicherzustellen, dass die Ergebnisse die Unternehmen erreichen. Daher müssen die im Antrag genannten Umsetzungsmaßnahmen und ihre tatsächliche Umsetzung im Mittelpunkt stehen. Je nach Art des Projekts müssen die erforderlichen Schritte im Antrag dargelegt und im Anschluss an das Pro-

jekt durchgeführt werden. Daher sollten die Darlegungen im Projektantrag einen verpflichtenden Charakter erhalten. Falls zusätzliche finanzielle Mittel dafür erforderlich sind, können diese durch die Forschungsvereinigungen bzw. Forschungsstellen bei der AiF beantragt werden. Die Transfererfordernisse können sich im Laufe des Projekts verändern. Daher sollte die Möglichkeit bestehen, die Liste der Transfermaßnahmen zum Abschluss des Projekts zu aktualisieren.

Vorschlag 6

Erfassung von Indikatoren, die Aussagen über die realen Transferprozesse ermöglichen, auf Ebene der Projekte und Forschungsvereinigungen im Rahmen eines Monitorings (vgl. Vorschläge in Punkt 4 unten). Sie sollten nicht nur während des Projekts, sondern auch nach Projektabschluss erfasst werden. Diese sind:

- Unternehmensmittel: Getrennter Ausweis von 1) Geldleistungen; 2) Sach- und Dienstleistungen; 3) Aufwendung für die Bereitstellung von Versuchsanlagen; 4) Aufwendungen für Mitglieder des projektbegleitenden Ausschusses.
- Anwesenheit von Unternehmensvertretern/ KMU-Vertretern auf den PA-Sitzungen.
- Im Anschluss an die Veröffentlichung der Projektergebnisse: Erfassung der Zugriffe auf die Internetseiten. Bei einem Zugriff sollte das Ausfüllen eines kurzen Fragebogens zur Zugehörigkeit zu einer Nutzergruppe, zu Motiven und zu der beabsichtigten Ergebnisnutzung verpflichtend gemacht werden.
- Durchführung von Transfermaßnahmen: Art, Umfang und Teilnehmer.
- Versand der ausführlichen Projektberichte an Interessenten, soweit diese nicht über die Internetpräsentation heruntergeladen werden können.
- Beratungsgespräche in den FV, Fst und Projektteams mit an den Projekten interessierten Unternehmensvertretern.

Begründung

Über den Transfererfolg der AiF insgesamt und einzelner Forschungsvereinigungen gibt es bislang nur wenige belastbare und repräsentative Informationen. Einiges hierzu hat die erweiterte Erfolgskontrolle beigesteuert. Insgesamt besteht allerdings ein Defizit an relevanten Informationen, die einen vollständigeren Überblick liefern könnten. Die Erfassung der Maßnahmen und von Indikatoren des Transfererfolgs ermöglicht es, ein klareres Bild von

den laufenden Transferprozessen und auftretenden Problemen bzw. Mängeln im Transfermanagement zu bekommen. Durch das Ansetzen an den Schwachstellen kann das Programm gezielt weiter entwickelt werden.

Vorschlag 7

Ein Teil der zukünftigen Fördersumme sollte für Transferaktivitäten zur Verfügung stehen. Diese Mittel sollten entsprechend den EU-Vorgaben (Anteilfinanzierung) projektbezogen (ggf. auch für mehrere zusammen) von den Forschungsvereinigungen beantragt werden können. Dafür ist eine getrennte Antragsprozedur einzurichten.

Der mögliche Verwendungszweck sollte nicht von vorneherein stark eingeschränkt werden, um den Forschungsvereinigungen die Möglichkeit zu geben, die Transfermaßnahmen auf die Adressatengruppe „zuzuschneiden".

Begründung

In einigen Forschungsvereinigungen werden bereits intensiv Transfermaßnahmen durchgeführt, in anderen in geringerem Maße. Ein möglicher (aber nicht der einzige) Grund für das Unterbleiben von erforderlichen Anstrengungen zum Technologietransfer ist, dass finanzielle Mittel erforderlich wären, die über die finanziellen Möglichkeiten einzelner Forschungsvereinigungen hinausgehen. Die Durchführung von Technologietransfermaßnahmen erfordert in vielen – bei weitem nicht allen – Fällen Aufwendungen, die über die „übliche" Verpflichtung zur Publikation und Verbreitung der Ergebnisse hinausgehen. Dazu gehört die Erstellung von „Werbematerial" zu den Ergebnissen der Forschung, mit denen auf die Kunden (die adressierten Unternehmen) zugegangen werden kann. Als weitere Maßnahmen sind z.B. Messestände der FV zu erwähnen etc.

Vorschlag 8

Die Forschungsvereinigungen sollen „best practices" der wirtschaftlichen Umsetzung von Ergebnissen der Förderung und des Technologietransfers identifizieren und einen gegenseitigen Austausch über Erfahrungen pflegen. Die „best practices" sollten in einer Broschüre zur Nutzung von IGF-Ergebnissen in Unternehmen und den dafür verfolgten Anstrengungen zusammengefasst werden.

Begründung

In vielen Fällen besteht sicherlich eine gewisse Hilflosigkeit bei den Forschungsvereinigungen in der Hinsicht, dass man nicht genau weiß, wie man die Ergebnisse der Förderung „zu den Unternehmen bekommt". Ist es überhaupt möglich und sinnvoll, dafür größere Anstrengungen zu unternehmen? Um das Bewusstsein für die Problematik zu stärken, sollte ein Erfahrungs- und Wissensaustausch zwischen den Forschungsvereinigungen in Gang gesetzt werden.

Vorschlag 9

Es sollten gezielt Maßnahmen zur Verbesserung der Sichtbarkeit des Programms nach außen und des BMWi als Geldgeber durchgeführt werden. Wir schlagen als erste Maßnahmen vor:

- Wie die meisten anderen Mittelstandsförderprogramme sollte auch die AiF auf den Webseiten zur IGF einen Flyer zum IGF-Programm als pdf-Dokument anbieten. Dieser Flyer mit dem Logo des BMWi sollte selbstverständlich auch als Druckwerk zum Verteilen vorliegen.

- Verpflichtung der Forschungsstellen, kurze (1-2seitige), gut lesbare **nicht-technische** Beschreibungen der Projektergebnisse für interessierte Unternehmen als Adressaten zu erstellen und diese aktiv bei den Unternehmen zu verbreiten.

Begründung

Der Bekanntheitsgrad der industriellen Gemeinschaftsforschung bei den Adressaten der Projekte, den innovativen Unternehmen des Verarbeitenden Gewerbes aber auch den innovativen Dienstleistungsunternehmen, lässt, wie die bisherigen Ergebnisse der erweiterten Erfolgskontrolle zeigen, zu wünschen übrig. Die AiF sollte deshalb aktiv daran arbeiten, dass sich dies in den nächsten Jahren verbessert.

Vorschlag 10

Vereinheitlichung der Vorgaben hinsichtlich des Ergebnistransfers für Zutech-Projekte und sonstige Projekte. Im Einzelnen: Der bislang in den Zutech-Projekten verpflichtende Plan zum Ergebnistransfer in die Wirtschaft

und zur Finanzierbarkeit der Umsetzung geht in die richtige Richtung, wobei ein „Abspecken“ möglich und sinnvoll ist.

Sie sollte eine Darstellung erhalten, welchen Beitrag das entsprechende Projekt zum Innovationsgeschehen leistet und wie sich daraus die erforderlichen Transfermaßnahmen ableiten (etwa: Projekt der angewandten Grundlagenforschung, weitere Anschlussprojekte erforderlich (Frage: welche?), oder: vorwettbewerbliches anwendungsorientiertes Projekt, an das unmittelbar FuE in den Unternehmen anschließen kann).

Darauf aufbauend muss eine begründete Beschreibung erfolgen, welche Transfermaßnahmen sich daraus ergeben und geplant/ durchgeführt werden.

Unser Vorschlag für die entsprechende Passage in der Gliederung des Antrags lautet:

5. Beabsichtigter Transfer der Forschungsergebnisse

5.1 Weg zur Umsetzung in den Unternehmen

Wer sind die Adressaten des Projekts (welche Unternehmen bzw. welche Unternehmensgruppe)?
Welchen Nutzen stiftet das Projekt? Worin wird letztlich der wirtschaftliche Nutzen liegen?
Welcher Weg ist geeignet, um die Ergebnisse zu den Adressaten zu bekommen?
Wie sieht ein realistischer Zeitrahmen aus?
Sind (insbesondere im Fall von Projekten, die eher der anwendungsorientierten Grundlagenforschung zuzurechnen sind) weitere öffentlich finanzierte Projekte erforderlich, um die Ergebnisse für Unternehmen interessant zu machen? Welche Wege sollen dabei beschritten werden?

5.2 Beabsichtige Transfermaßnahmen (über die ohnehin bestehenden Verpflichtungen hinaus)

Hier können die bislang in Punkt 5.1 aufgeführten Möglichkeiten genannt werden.

Im Monitoring-System (vgl. hierzu die Vorschläge 13 und 14) sollten auch regelmäßig solche Projektmerkmale erfasst werden, welche für den Ergebnistransfer von Belang sind, z.B. Anwendungsnähe (-ferne) des Projekts, geschätzte Zahl potenzieller Nutzer der Ergebnisse, geschätzte Entwicklungskosten bei Weiterentwicklung zur Anwendungsreife.

Begründung

Die Ausführungen zum Ergebnistransfer in den Forschungsanträgen und die Bewertungsrichtlinien für die Gutachter tragen den möglichen unterschiedlichen Transferprozessen zu wenig Rechnung. Das unternehmensorientierte (also kundenorientierte) Denken sollte mehr in die Beantragung hineingetragen werden, ohne einen überflüssigen zusätzlichen Aufwand bei der Beantragung zu schaffen. Die Regelung bei den Zutech-Projekten stellt, auch wenn sie teilweise in der AiF und den Forschungsvereinigungen kritisch gesehen wird, einen Schritt in die richtige Richtung dar. Die Erfordernisse des Technologietransfers unterscheiden sich sehr deutlich bei den einzelnen Projekten. Dennoch sollte aus dem Antrag nicht nur hervorgehen, welche Maßnahmen geplant sind, sondern ebenfalls, wie sich der Weg zur möglichen Umsetzung in den Unternehmen darstellt. Es sollte somit auch begründet werden, warum die vorgeschlagenen Transfermaßnahmen geeignet sind.

3. Antrags-, Begutachtungs- und Bewilligungsverfahren

Die Attraktivität von Technologieprogrammen für die angesprochenen Adressatengruppen hängt nicht zuletzt davon ab, dass effiziente Verwaltungsstrukturen durchgesetzt werden und – angesichts sich verkürzender Innovationszyklen – die zwischen der Formulierung der Projektidee und dem Anlauf des Projekts liegende Spanne verkürzt wird. Hierbei steht natürlich das berechtigte Interesse des Förderers an einer korrekten administrativen Abwicklung des Programms in einem objektiven Gegensatz zum Interesse der von der Förderung profitierenden Forschungsvereinigungen, Forschungsstellen und Forscher sowie auch der partizipierenden Unternehmen an einer möglichst raschen und unbürokratischen Ausgestaltung der Verwaltungsvorgänge. Anliegen aller Beteiligten sollte es sein, hier eine möglichst „optimale“ Lösung zu finden.

Vorschlag 11

Es sollten systematische Anstrengungen zur Verkürzung des Zeitbedarfs für das Antrags- und Bewilligungsverfahren unternommen werden. Dabei sollte überprüft werden, an welchen Stellen des Antrags- und Bewilligungsverfahrens noch Potenziale zur Reduzierung des Zeitaufwands bestehen. Auf der Basis von durchschnittlichen Werten für den Zeitbedarf – wenn diese verfügbar sind – würde es durchaus Sinn machen, sich ehrgeizige Ziele zu setzen (etwa eine Halbierung des Zeitbedarfs für die Antrags- und Bewilli-

gungsverfahren). Bei der Verkürzung der Zeiträume sollte die AiF eine zentrale Funktion einnehmen. Im Einzelnen ist zu prüfen:

- wie eine Verkürzung der Zeitspannen von der Projektidee bis zur Beantragung der Projekte in den Forschungsstellen bzw. Forschungsvereinigungen möglich ist (welche „best practices" existieren hierbei in den einzelnen Forschungsvereinigungen),
- ob Gutachter, die zeitlich zu stark belastet sind, durch andere ersetzt werden können,
- ob Begutachtungssitzungen vermehrt durch Entscheidungsverfahren im Email-Umlauf ersetzt werden können,
- ob durch eine zeitliche Abstimmung von Terminen ein schnellerer Durchlauf von Projektanträgen gesichert werden kann,
- ob in dem komplexen Ablaufschema des Antrags- und Bewilligungsverfahrens noch Vereinfachungsmöglichkeiten existieren,
- wie der Zeitraum von der Bewilligung bis zum Mittelabfluss an die Letztempfänger verkürzt werden kann,
- ob bestimmte Anforderungen detailliert nachgewiesen werden müssen oder hier Pauschalzuweisungen ausreichen.

Begründung

Der erforderliche Zeitraum für die Antrags- und Bewilligungsverfahren ist nach Eindrücken aus der erweiterten Erfolgskontrolle im Vergleich zu anderen FuE-Förderprogrammen für mittelständische Unternehmen lang. In der Vergangenheit wurden Anstrengungen zur Verkürzung des Antrags- und Bewilligungsverfahrens unternommen. Gleichzeitig bestehen sicherlich noch weitere Potenziale zur Verkürzung der Zeiträume. Die Hoffnung bzw. Erwartung ist, dass durch schlankere und effizientere Verwaltungsverfahren die Attraktivität der IGF für die Unternehmen des innovativen Mittelstands steigt.

Hilfreich wäre evtl. die Durchführung eines Workshops, in dem die beteiligten Seiten gemeinsam die Möglichkeiten einer Verkürzung der prozeduralen Abläufe ausloten. Bei Bedarf könnte eine solche Veranstaltung nach einer Absprache über durchzuführende Maßnahmen wiederholt werden, um deren Erfolg zu überprüfen.

Vorschlag 12

Eine Anpassung der Gutachterfragebögen und Vereinheitlichung der Fragebögen für Projekte im Normalverfahren und von Zutech-Projekten wäre sinnvoll. Im Gutachterfragebogen sollten die beiden Abschnitte zum Tech-

nologietransfer denselben Stellenwert wie der Nutzen und die wirtschaftliche Bedeutung für KMU erhalten: Unser Vorschlag ist, für beide Aspekte jeweils 8 Punkte zu vergeben. Die Gutachter sollten sowohl den genannten Weg für die Umsetzung als auch die beabsichtigten Transfermaßnahmen in Hinblick auf ihre Plausibilität überprüfen. Auch hier entfällt die getrennte Bewertung des Ergebnistransfers bei Zutech-Projekten.

Unser Vorschlag für die Bewertung des Technologietransfers im Gutachterfragebogen lautet:

III. Technologietransfer

1. Weg zur Umsetzung in den Unternehmen (4 Punkte)

Zentrale Frage: Ist der Weg hin zur Umsetzung plausibel dargestellt?
- *Wer sind die Adressaten des Projekts (welche Unternehmen bzw. welche Unternehmensgruppen)?*
- *Welchen Nutzen stiftet das Projekt konkret? Worin wird letztlich der wirtschaftliche Nutzen liegen?*
- *Welcher Weg ist geeignet, um die Ergebnisse an die Adressaten zu vermitteln?*
- *Wie sieht ein realistischer Zeitrahmen aus?*
- *Sind (im Fall von Grundlagenforschungsprojekten) weitere öffentlich finanzierte Projekte erforderlich, um die Ergebnisse für Unternehmen interessant zu machen? Welche Wege sollen dabei beschritten werden?*

2. Beabsichtige Transfermaßnahmen (4 Punkte)

- *Sind die geplanten Transfermaßnahmen geeignet, um sicherzustellen, dass die Adressaten hinreichend über die Projektergebnisse informiert werden?*

Begründung

Die Gutachter sollten sowohl den genannten Weg für die Umsetzung als auch die beabsichtigten Transfermaßnahmen in Hinblick auf ihre Plausibilität überprüfen. Nur so ist sichergestellt, dass auch in der Beantragungsphase nicht nur der Nutzen des Projekts für KMU, sondern auch die Umsetzung der Projektergebnisse von vorneherein im Blick behalten wird. Dabei soll es zu keiner Diskriminierung von Projekten kommen, die eher Grundlagencharakter haben und weiter von der direkten Nutzung in mittelständischen Unternehmen entfernt sind. Dennoch gilt auch für diese Projekte: Es sollte von vorneherein im Blick behalten werden, wie über spätere Anschlusspro-

jekte eine Umsetzung der Ergebnisse eines „Projektstrangs“ in den Unternehmen möglich ist.

4. Monitoring

Das BMWi und die Institutionen der Gemeinschaftsforschung haben ein vitales Interesse daran, möglichst zeitnah und detailliert Aufschluss über die Prozessabläufe und (messbaren) Ergebnisse der IGF zu erhalten. Ein gutes Monitoring-System ist elementare Voraussetzung dafür, dass die Handelnden über Stärken, Schwächen und Verbesserungsmöglichkeiten des Programms informiert sind. Nicht zuletzt gründen Evaluationen staatlicher Programme stets in erster Linie auf Informationen, welches das Monitoring des jeweiligen Programms liefert. Die technischen Möglichkeiten für den Aufbau eines zugleich kostengünstigen und leistungsfähigen Monitoring-Systems haben sich im Zuge der Verbreitung der modernen Informations- und Kommunikationstechnologien in jüngster Zeit enorm verbessert. Die hier bestehenden Möglichkeiten sollten voll ausgeschöpft werden. Dies ist offensichtlich bislang nicht der Fall.

Vorschlag 13

Es wird vorgeschlagen, ein datenbankbasiertes elektronisches Informationssystem zur IGF aufzubauen, welches bei der AiF angesiedelt ist und von dieser betreut wird. Über ein webbasiertes Intranet sollten alle Forschungsvereinigungen sowie auch das zuständige Referat des BMWi Zugang haben. Zugleich sollten über ein Modul ausgewählte Informationen über die IGF-Projekte für externe Nutzer – d.h. vor allem die mittelständischen Unternehmen als Adressaten der Förderung – verfügbar gemacht werden (Näheres hierzu in Vorschlag 14). Die Zugriffsrechte auf die Datenbestände für die angeschlossenen Einrichtungen sind entsprechend dem jeweiligen Zuständigkeitsbereich zu regeln. Praktische Beispiele aus Wirtschaft und Verwaltung zeigen, dass die Einrichtung eines solchen elektronischen Informationssystems sowohl unter Praktikabilitäts- als auch unter Kosten- und Sicherheitsaspekten keine unüberwindbaren Schwierigkeiten entgegenstehen (vgl. hierzu die Anlagen im Anhang).

Das elektronische Informationssystem sollte alle relevanten Informationen zum Programmgeschehen integrieren und dabei auch solche Informationen zu den Projekten enthalten, die bislang nur in schriftlicher Form vorliegen (z.B. Gutachtervoten im Volltext in Memofeldern) bzw. die bislang überhaupt nicht zentral erfasst worden sind (z.B. PA-Mitglieder, PA-Tagungstermine, Informationen zum Transfer). Die Datenbank sollte den

FV auch die Möglichkeit eröffnen, projektrelevante Informationen wie z.B. Zahlungsanforderungen sowie Endverwendungsnachweise online einzugeben. Die Eingabe und die Datenpflege sollten somit in wesentlichen Teilen dezentralisiert, nämlich durch die Forschungsvereinigungen erfolgen. Der AiF käme die Funktion der Konzipierung sowie der Pflege des Gesamtsystems zu. Letztere schließt die zeitnahe Eingabe zentraler Daten, die Kontrolle und Koordinierung der Datenpflege durch die FV, die Überwachung der Funktionstüchtigkeit des Systems, seine technische „Optimierung" und den Schutz des Systems gegen Zugriffe unberechtigter Dritter ein.

Im Einzelnen wären folgende Schritte zu realisieren:

1. Zunächst sollte ein Fachkonzept entwickelt werden, das die Aufgaben und Inhalte sowie Unterteilungen der Datenbank definiert.

2. Im elektronischen Informationssystem sollten die Angaben zu den Projekten besondere Bedeutung haben. Es sollte ein „Projektstammblatt" entwickelt werden, das definiert, welche Informationen in welcher Struktur und zu welchen Zeitpunkten einzugeben sind.

3. Durch die Einrichtung bestimmter Bereiche, die jeweils mit oder ohne Passwort zugänglich sind, kann sichergestellt werden, dass jeweils nur die Berechtigten Zugriff haben.

4. Bereiche, die ein solches integriertes elektronisches Informationssystem umfassen sollte, sind u.a.

- Projekttitel, Laufzeit, Projektabschluss,
- Kurzbeschreibung (Abstract) zum Projektinhalt,
- evtl. die vollständigen Forschungsberichte,
- aussagekräftige und leicht verständliche Kurzbeschreibungen der Projektergebnisse bei abgeschlossenen Projekten,
- detaillierte Schlagworte zu dem Projekt und eine effiziente Suchfunktion, die auch für wenig geübte Nutzer schnelle Zugriffe auf abgeschlossene wie laufende Projekte ermöglicht,
- Angaben zu den möglichen technischen Anwendungsbereichen und potenziellen Nutzerbranchen der Projekte,
- Ansprechpartner bei FV und Fst für die jeweiligen Projekte,
- Informationen der FV und Fst zu Verbreitungsmaßnahmen,
- Antragsformulare,
- Abrechnungsformulare,
- Gutachter, Adresse, Fachrichtung, Funktion,
- Gutachten im Volltext (in Memofeldern),
- Mitglieder der PA, Sitzungstermine und Teilnehmerlisten der PA-Sitzungen,

- projektbezogene Veranstaltungen der AiF, FV und Fst,
- Abrechnungsdaten der AiF,
- allgemeine Dokumente zur IGF/AiF,
- Auswertungsmodule für die Berichterstattung zur Programmabwicklung durch die AiF.

Begründung

Derzeit existiert kein elektronisches Informationssystem der angesprochenen Art und auch keine umfassende Datenbank zu den IGF-Aktivitäten. Die bisher existierende Datenbank steht nur AiF-intern zur Verfügung. Entsprechende Planungen wurden nach unseren Informationen einstweilen eingestellt. Die bisher (für die Projektabwicklung) eingesetzten ACCESS-Datenbanken stellen Partiallösungen dar, die technisch eher als veraltet einzustufen sind. Für die hier vorgeschlagene Lösung kämen z.B. die Datenbankprogramme von Oracle oder SAP in Betracht. Wichtig ist, dass bei einer Modernisierung der elektronischen Datenverwaltung die gleiche Software auf zentraler Ebene (AiF) und dezentraler Ebene (FV) Anwendung findet und nicht – im ungünstigsten Fall – mit 103 unterschiedlichen, nur bedingt kompatiblen Softwarelösungen gearbeitet wird. Das hier vorgeschlagene integrierte elektronische Informationssystem könnte in erheblichem Maße zur Verbesserung des Monitoring in der IGF beitragen und auch zu effektiveren Verwaltungsabläufen, insbesondere an den Schnittstellen von AiF und FV sowie von BMWi und AiF.

Vorschlag 14

Beim Aufbau der integrierten Datenbank sollte die Möglichkeit genutzt werden, diejenigen Projektinformationen, welche für die Adressaten der Förderung von Interesse sind, über das Internet Externen zugänglich zu machen. Hier sollte sich jede/r Interessierte ständig über durchgeführte und laufende Projekte informieren können. Mit anderen Worten, es sollte eine (relativ eng begrenzte) Teilmenge der in der Datenbank gespeicherten Daten über das Internet allgemein und leicht zugänglich sein.

Auszuweisen wären hier insbesondere:

- Titel der durchgeführten und laufenden Projekte,
- Zeitraum der Durchführung und Zeitpunkt des Abschlusses,
- Projekt-Kurzbeschreibung (Abstract),
- bei abgeschlossenen Projekten ein aussagekräftiger, leicht verständlicher Ergebnisbericht,

- zuständige FV mit Ansprechpartner,
- durchführende Fst mit Ansprechpartner,
- Ansprechpartner des Projektteams,
- Schlagworte zu den Projektinhalten,
- Diskussionsplattformen zu den einzelnen Projekten,
- Fragebogen für die Nutzer der Datenbank,
- Hinweise zu anderen Forschungsförderprogrammen (evtl. in Kombination mit den Projektberichten: man könnte potentielle Nutzer hier darauf hinwiesen, mit welchen anderen Programmen z.B. Weiterentwicklungen finanziert werden können).

Die Indexierung der Projekte per Schlagworte sollte externen Nutzern jederzeit die Möglichkeit geben, sich über die Entwicklung in dem sie speziell interessierenden Technologiefeld auf einfache und rasche Art zu informieren. Querverweise zu den FV und Fst sollten vertieften Recherchen bei den FV und Fst ermöglichen.

Begründung

Die AiF veröffentlicht in ihren Jahresberichten Informationen über die im jeweiligen Zeitraum abgeschlossenen Projekte. Diese Informationen sind auch in elektronischer Form – auf CD – erhältlich. Externe Interessenten in den Unternehmen können auf dieser Basis allerdings nur dann ein vollständiges Bild über das Projektgeschehen in dem sie interessierenden Technologiefeld gewinnen, wenn sie sich selbst die relevanten Informationen aus den einzelnen Berichtsjahrgängen zusammenstellen. Die Erfassung des Projektgeschehens in einer relationalen Datenbank schafft ganz andere Möglichkeiten des Zugangs zum Projektgeschehen, bedeutet mithin eine neue Qualität der elektronischen Information über die industrielle Gemeinschaftsforschung.

Hier könnte man einwenden, dass das elektronische Sicherheitsrisiko der Zugänglichmachung einer (kleinen) Teilmenge der im aufzubauenden integrierten Datenbanksystem der IGF für Internetnutzer ohne spezielle Sicherheitsvorkehrungen mit einem zu großen Risiko des Zugriffs durch externe Benutzer auf die internen Datenbestände behaftet sei. Prinzipiell stellt die Abschottung der für die Öffentlichkeit zu sperrenden Bereiche datentechnisch kein unlösbares Problem dar. Die auf dem Markt befindlichen großen Datenbanksysteme wie diejenigen von Oracle und SAP sind dazu in der Lage, entsprechende Sicherheitsvorkehrungen zu treffen. Erinnert sei an einschlägige Erfahrungen mit Internetdatenangeboten, z.B. an das Datenportal GENESIS-Online des Statistischen Bundesamtes oder die Online-Banking-Angebote der Geschäftsbanken. Dass hierbei ein Restrisiko bleibt,

soll nicht geleugnet werden. Falls die Risiken den Verantwortlichen der AiF zu hoch erscheinen, käme alternativ auch die Bereitstellung einer separaten Teildatenbank für die interessierte Öffentlichkeit in Betracht. Dies wäre allerdings eine kostspieligere und weniger elegante Lösung des Sicherheitsproblems.

Der AiF käme als Initiator und Hüter des datenbankbasierten elektronischen Informationssystems eine herausragende Funktion zu. Dies hätte den Vorteil, dass für das Anliegen der Gemeinschaftsforschung verstärkt auf zentraler Ebene geworben werden könnte und „IGF“ und „AiF“ als Marken verbreitet werden könnten. Nach Auskunft der FV wenden sich an Projektergebnissen interessierte Unternehmen bislang in erster Linie an die FV und nicht an die AiF. Dies hängt wahrscheinlich damit zusammen, dass die IGF als „Marke“ nur wenig bekannt ist und es sich daher bei den Anfragern und Anwendern häufig um „Insider“ handelt. Falls die IGF bzw. AiF besser als Marken bekannt wären, dürften auch die Anfragen an die AiF zunehmen. Dies spricht für eine Konzentration wesentlicher Informationen bei der AiF.

Vorschlag 15

Die Meilensteine des Antrags- und Bewilligungsverfahrens und die zugehörigen Zeiträume sollten für die einzelnen Projekte präziser im Monitoring-System erfasst werden.

Begründung

Eine systematische Erfassung von der Ideengenerierung über den Antragsversand, die Entscheidung über die Antragseinreichung (Beginn der Phase 2 des Antrags- und Bewilligungsverfahrens) bis zum Start des Projekts der verstreichenden Zeiträume findet nicht statt. Die Erfassung der Informationen zu den Zeiträumen in den Antrags- und Bewilligungsverfahrens würde die Errechnung von projektdurchschnittlichen Zeiten ermöglichen und zugleich die Erfolgsmessung für Anstrengungen zur Verkürzung des Zeitraums für das Antrags- und Bewilligungsverfahren erlauben. Gleichzeitig würden die erfassten Daten wichtige Informationen für ggf. noch vorhandene Potenziale zur Verringerung des Zeitaufwands liefern.

5. Ausgewählte systemische Aspekte

Anders als viele sonstige strukturpolitische Programme des Bundes verfügt die IGF über ein Netz von Institutionen – AiF, 103 FV, Fst –, welches sich, beginnend in den 1950er Jahren, sukzessive nach dem Selbstorganisationsprinzip herausgebildet hat. Die AiF ist vor diesem Hintergrund im Kontext der IGF kein „normaler" Projektträger, sondern hat auch im Sinne des Programms ein „institutionelles" Eigenleben entwickelt. Änderungen der bestehenden Organisationsstrukturen können nicht von außen verordnet werden, sondern müssen von den Institutionen der Gemeinschaftsforschung getragen und verantwortet werden. Die Betrachtung systemischer Aspekte der IGF trägt diesem Tatbestand Rechnung.

Vorschlag 16

Die Auswirkungen der sukzessiven Einführung des Wettbewerbsverfahrens für die Hälfte der Projektmittel auf die Verteilung der Mittel auf die FV, Branchen und Technologiefelder sollten zeitnah untersucht werden. Falls das veränderte Begutachtungssystem seine Aufgabe erfüllt, sollte der „wettbewerbliche" Bereich bis 2010 wesentlich (bis zu drei Viertel) ausgedehnt und die Zutech-Projekte in die wettbewerbliche Mittelvergabe aufgenommen werden.

Begründung

Die Stärkung des Wettbewerbsverfahrens führt dazu, dass die von den Gutachtern am besten bewerteten Projekte ausgewählt werden, also die Effizienz des Auswahlverfahrens erhöht wird. Das Gewicht der Gutachergruppe und damit der Gutachtervoten im gesamten Auswahlprozess steigt stark an. Gleichzeitig führt dieses Verfahren zu einem erhöhten Wettbewerbsdruck auf die Forschungsvereinigungen, die eine Straffung (etwa die Zusammenlegung thematisch näher verwandter Forschungsvereinigungen) zur Folge haben kann.

Vorschlag 17

Die Zusammenarbeit zwischen thematisch verwandten Forschungsvereinigungen sollte intensiviert und Fusionen zwischen FV, welche einander über-

lappende oder angrenzende Forschungsfelder besetzen, durch Gremien der AiF ermutigt werden.

Sollten weitergehende organisatorische Schritte sich zunächst als zu schwierig erweisen, können zumindest regelmäßige Treffen von Vertretern von Forschungsvereinigungen initiiert werden, die überschneidende Fragestellungen bearbeiten. Ziel dieser Treffen sollte es sein, Kontakte zu knüpfen und Informationen über Projekte auszutauschen, die für die jeweils anderen Forschungsvereinigungen und deren Mitgliedsunternehmen von Interesse sind. Die AiF sollte die hier geforderte Kooperation systematisch unterstützen.

Begründung

Im Rahmen der erweiterten Erfolgskontrolle ist deutlich geworden, dass es zwischen den Forschungsvereinigungen teilweise überlappende Themenfelder gibt und der Austausch über Projekte zwischen den Forschungsvereinigungen, also der AiF-interne Wissenstransfer, verbesserbar ist. Solche Begegnungen finden bereits sporadisch statt. Eine Institutionalisierung bei eng verwandten Forschungsfeldern erscheint sinnvoll.

Anhang

Anlage 1

Monitoringsystem für die IGF: Architektur, Kosten, Sicherheit – Ein Beispiel für ein vergleichbares DV-Gesamtkonzept

Bearbeiter: Dr. Werner Friedrich

Datum: 3. April 2007

Das derzeitige DV- und Monitoringsystem der AIF/IGF ist verbesserungsbedürftig. Daher wird in den Vorschlägen 13 und 14 (vgl. S. 18ff.) angeregt, ein elektronisch basiertes Informationssystem zu entwickeln, das alle relevanten Funktionen in sich vereinigt, d.h. Information der Öffentlichkeit, laufendes Programmmonitoring und -controlling, finanzielle Beteiligung der FV sowie der Fst, Finanzabwicklung, Abrechnung/Verwendungsnachweise der Projekte etc.

Das System sollte Internet-basiert sein und nach Modulen getrennt werden. Für diese Module gibt es unterschiedliche Lese- und Schreibrechte. So kann z.B. die Öffentlichkeit auf die Datenbank der abgeschlossenen und laufenden Projekte sowie weiterführende Informationen zur IGF zugreifen, die FV haben z.B. Zugriff auf ihre Finanzdaten, Gutachterverzeichnisse etc. Projektverantwortliche können z.B. ihre Verwendungsnachweise/Abrechnungen online eingeben und auch lesen. Weiterhin können die Projektverantwortlichen Informationen über ihre Vorhaben einstellen, z.B. Ergebnisse, Zwischenberichte, Informationen über Veranstaltungen und andere Verbreitungsmaßnahmen.

Durch eine klar definierte Rechteverwaltung – über entsprechende Nutzerklassen und dazugehörige Passwörter – kann sichergestellt werden, dass keine Unbefugten die Daten manipulieren oder lesen können.

Dazu ist ein umfassendes Datensicherheitskonzept erforderlich, dass auch die Server vor unbefugten Zugriffen sichert. In der Anlage ist beispielhaft ein solches Konzept der Firma Proximity (gehört zu dem Beratungs- und Internetdienstleistungsunternehmen BBDO Germany) dargestellt.

Für solche DV-Gesamtkonzepte gibt es in Deutschland viele Beispiele. Nachstehend soll ein System, das Dr. Friedrich für die Abwicklung des Eu-

ropäischen Sozialfonds in Deutschland (ESF) im Auftrag des Bundesministeriums für Arbeit und Soziales entwickelt hat und seit 2001 betreibt, beispielhaft beschrieben werden.

- Das System ist web-basiert (https://www.esf-de.de).
- Das System wird bei einem externen Dienstleister gehostet (Proximity/BBDO). Diese stellt die permanente Verfügbarkeit, die laufende Datensicherung sowie den Schutz vor unbefugten Zugriffen sicher.
- Auf dieses System haben Zugriff:
  - das Bundesministerium für Arbeit und Soziales,
  - das Bundesministerium für Bildung und Forschung,
  - das Bundesministerium für Familie, Frauen, Senioren und Jugend,
  - die Bundesagentur für Arbeit,
  - alle 16 Bundesländer,
  - weitere nachgeordnete Bundesbehörden,
  - die Projektträger, die in Deutschland im Rahmen der ESF-Bundesprogramme Projekte durchführen .
- Das System beinhaltet folgende Daten:
  - „Stammblätter“ zu Projekten, geförderten Unternehmen und Personen, die i.d.R. von den Projektträgern eingepflegt werden,
  - aggregierte Finanzdaten, differenziert nach den oben genannten Institutionen (Ministerien, Bundesbehörden),
  - die finanziellen Plandaten (Jahrestranchen) nach verschiedenen Interventionszielen,
  - Auswertungsroutinen zur finanziellen Förderung, geförderten Unternehmen und Personen,
  - nicht enthalten sind derzeit ein für die Öffentlichkeit zugänglicher Bereich sowie die Finanzverwaltung auf Ebene der Projekte, solche Systeme mit Finanzdaten für Projekte betreiben z.B. die Länder NRW und M-Vorpommern (wurden ebenfalls von Proximity entwickelt).

- Kosten des Moduls:
  - Einmalige Entwicklungskosten: 260.000 € (netto)
  - Einmalige Programmierung ergänzender Module 120.000 €
  - Hosting pro Jahr 12.000 € p.a.
  - Softwarelizenzen pro Jahr 3.500 € p.a.
  - Technische Anpassungen 5.000 € p.a.

Das System enthält „zu schützende“ Finanzdaten und personenbezogene Daten. Es wurde vom Bundesdatenschutzbeauftragten geprüft und abgenommen.

Falls gewünscht, können wir dem BMWi dieses System in allen Bereichen vorführen, da wir über unbeschränkte Lese- und Schreibrechte verfügen.

Wir schätzen, dass ein vergleichbares System für die IGF/AiF folgende Kosten verursachen würde:

- Einmalige Entwicklung sowie Ergänzungen 650.000 € (netto)
- Laufende jährlich anfallende Kosten 50.000 €

Erforderlich ist zudem Personal bei der AiF, das z.B. die Plausibilität der Eingaben prüft und neue Dokumente – z.B. Richtlinien, Forschungsreports etc. – in die Datenbank einstellt.

Anlage 2

IT-Grundschutzhandbuch
Proximity

Inhaltsverzeichnis für IT-Grundschutzhandbuch Proximity

Einleitung

Datenschutz als rechtliche und gesellschaftspolitische Verpflichtung

Datenschutz und Datensicherheit sind mit Blick auf die modernen Informations- und Kommunikationstechnologien sowie den wachsenden wirtschaftlichen Wert personenbezogener Daten wichtige Grundpfeiler der Informationsgesellschaft. Im Zuge der Globalisierung und weltweiten Technisierung hat der Einsatz von luK-Technologien stark zugenommen. Auf Grund der hieraus resultierenden Gefahren für das verfassungsrechtlich anerkannte Recht auf informationelle Selbstbestimmung gewinnen Datenschutz und IT-Sicherheit immer mehr an Bedeutung.

Nicht nur Chancen und Gewinne sind mit der Nutzung modernster Datenverarbeitungstechnik verbunden, sondern auch Risiken für den Einzelnen, für Unternehmen und Behörden sowie für die Gesellschaft insgesamt. In einer multimedialen Welt, in der Computersysteme weltweit vernetzt sind, können personenbezogene Informationen in vielfältiger Weise erhoben, beliebig kombiniert, verändert und ausgewertet werden. Die Kontrollmöglichkeiten des Nutzers sind demgegenüber begrenzt. Datenschutz und das Vertrauen in den Persönlichkeitsschutz sind daher notwendig für die Akzeptanz der angebotenen Dienste.

Besonders bei multimedialen Anwendungen sind Datenschutz und Datensicherheit aus Sicht des Nutzers Qualitätsmerkmale und damit für die Anbieter Wettbewerbsfaktoren.

Fünf gute Gründe für einen modernen Datenschutz

- Datenschutz bedeutet grundrechtlich verbürgten Persönlichkeitsschutz.
- Der Schutz der Privatsphäre eines jeden Einzelnen ist im Zeitalter der Informationsgesellschaft unerlässlich.
- Datenschutz bedeutet im modernen Wirtschaftsleben einen Qualitäts- und Wettbewerbsfaktor.
- Datenschutz und Datensicherheit sind Wegbereiter für den E-Commerce.

Im Zuge der Globalisierung gewinnt der Datenschutz auch international zunehmend an Bedeutung.

Datenschutz, Datensicherheit und ordnungsgemäße Datenverarbeitung sollen alle Beteiligten vor Gefahren schützen und gleichzeitig Informationsfreiheit und Informationsgleichgewicht gewährleisten. Sie beinhalten gesetzliche Pflichten, die alle Unternehmen und Verwaltungseinheiten treffen, gleich welcher Größenordnung oder Branche.

Der Datenschutzbeauftragte (DSB)

Aufgaben des DSB

- Auf Einhaltung des BDSG und anderer Vorschriften über den Datenschutz hinwirken.
- Die ordnungsgemäße Anwendung der DV-Programme, mit deren Hilfe personenbezogene Daten verarbeitet werden, überwachen.
- Die bei der Verarbeitung personenbezogener Daten tätigen Personen schulen. Dies kann zum Beispiel in schriftlicher Form, durch Schulungsveranstaltungen oder auch durch Anregungen und Informationen im Rahmen von Dienstbesprechungen erfolgen.
- Jedermann auf Antrag die Angaben über Verfahren automatisierter Verarbeitungen in geeigneter Weise zur Verfügung stellen.
- Vor Beginn der automatisierten Verarbeitung kontrollieren, ob die Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweist.

Rechte und Pflichten

Der Beauftragte für den Datenschutz ist der Geschäftsführung unmittelbar unterstellt. Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei und darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Er ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird. Proximity ist verpflichtet, den DSB bei der Erfüllung der Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung der Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Dem DSB ist von der verantwortlichen Stelle eine Übersicht über die meldepflichtigen Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen. Der DSB ist über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten.

Externer Datenschutzbeauftragter für Proximity:

Herr Uwe Hagen
Eulenkamp 15
30989 Gehrden
Tel. 05108/922644; e-mail: hagen.u@t-online.de

Öffentliches Verfahrensverzeichnis

Öffentliches Verfahrensverzeichnis gemäß § 4g BDSG
Stand: 02/ 05

Name oder Firma der verantwortlichen Stelle	a) Proximity Group Germany GmbH b) Proximity I\Tec GmbH
Leiter der Verantwortlichen Stelle und der Datenverarbeitung	Geschäftsführer: zu a) Michael Schipper, Michael Warsönke, Martin Nitsche Zu b) Markus Keller Leiter DV: Guido Hein
Anschrift	Dorotheenstraße 64 22301 Hamburg
Zweckbestimmung der Datenerhebung, -verarbeitung, oder -nutzung	Gegenstand des Unternehmens ist der Betrieb einer Direkt-Marketing-Agentur und einer Werbeagentur mit umfassenden Service und einer Sales-Promotion-Agentur und einer Agentur für Öffentlichkeitsarbeit (PR). Die Gesellschaft kann sich an anderen Unternehmen beteiligen.
Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien	**Kundenverwaltungsverfahren(juristische Personen):** Ansprechpartner **Personalverwaltungsverfahren:** Personengruppen: Mitarbeiter, Datenkategorien: Adressdaten, Vertragsdaten, Abrechnungsdaten, Sozialversicherungsdaten, Bankverbindung, Telefongebühren(Mobil) **Lieferanten (juristische und natürliche Personen)** Adressdaten, Vertragsdaten, Umsatzdaten
Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	➢ externe Stellen bei Vorliegen vorrangiger Rechtsvorschriften ➢ öffentliche Stellen bei Vorliegen vorrangiger Rechtsvorschriften ➢ externe Auftragnehmer entsprechend § 11 BDSG ➢ externe Stellen auf Verlangen des Betroffenen
Regelfristen für die Löschung der Daten	Die Löschung erfolgt nach Ablauf der gesetzlichen Aufbewahrungsfristen
Geplante Datenübermittlung in Drittstaaten	nicht geplant

Das Sicherheitskonzept

Es sind IT-Sicherheitsziele definiert, damit angemessene Maßnahmen getroffen werden können. Für das Sicherheitskonzept werden berücksichtigt:

1) Rahmenbedingungen:

- Gesetze
- Verträge
- Kundenanforderungen
- Konkurrenzsituation

2) Zu schützende Werte:

- Know-how
- Betriebsgeheimnisse
- Mitarbeiterdaten
- Kundendaten

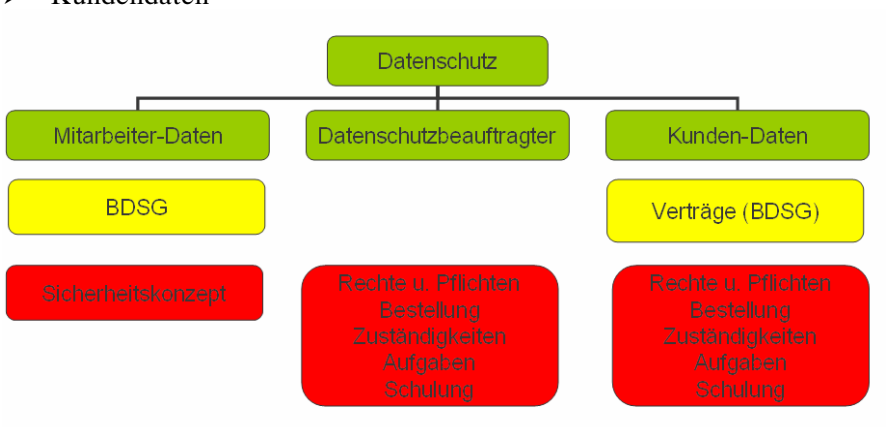


Abbildung: Trennung der zu schützenden Daten hinsichtlich Mitarbeiter- und Kundendaten

3) Mögliche Schadensfälle:

Siehe Kap. Notfallvorsorgekonzept

4) „Schutzbedarfsfeststellung“ (Bestandteil der Sicherheitsanalyse)

Es besteht ein Überblick über die wichtigsten Anwendungen und IT-Systeme und deren Schutzbedarf.

Eine regelmäßige Überprüfung des Schutzbedarfs hinterfragt, ob die Einstufung des Schutzbedarfs noch der aktuellen Situation entspricht.

Dabei orientiert sich Proximity an den drei Grundwerten der IT-Sicherheit:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Somit wird sichergestellt, dass die definierten Schutzziele und die hieraus abgeleiteten Sicherheitsmaßnahmen angemessen sind und den individuellen Gegebenheiten entsprechen.

Anlagen:

- Schutzbedarfsfeststellung in der IT-Systemtechnik

IT-Sicherheitsmanagement

Dieses Kapitel zeigt, wie das IT-Sicherheitsmanagement funktioniert und im laufenden Betrieb weiterentwickelt wird. Ein funktionierendes IT-Sicherheitsmanagement ist die wesentliche Grundlage für die Erreichung eines angemessenen Sicherheitsniveaus.

Die Unternehmensleitung hat die IT-Sicherheitsziele festgelegt und sich zu ihrer Verantwortung für die IT-Sicherheit bekannt. Alle gesetzlichen oder vertragsrechtlichen Gesichtspunkte sind berücksichtigt worden. Langfristig wird ein umfassendes Sicherheitsmanagement aufgebaut.

1) allgemeine Sicherheitsziele: Zusammenfassung der eigenen Unternehmensphilosophie in Sachen IT-Sicherheit. „Managementtauglich“ und von der obersten Leitungsebene verabschiedet.

2) detaillierte Sicherheitsziele: ausführliche technische Anforderungen und zugehörige Maßnahmen, ohne produktspezifische Aspekte oder Eigenschaften. Sicherheitsziele müssen somit nicht permanent geändert werden.

3) Konkrete Produkteinstellungen und verwendete Mechanismen.

   - Sobald sich ein eingesetztes Produkt geändert hat, werden Anpassungen vorgenommen.
   - Anforderungen, die mangels Produktfunktionalität oder fehlender Praktikabilität nicht umgesetzt werden können, werden nochmals überdacht oder es wird eine andere Lösung eingesetzt.

- Defizite bei der Umsetzung werden explizit festgehalten und alle Verantwortlichen informiert, um das entstandene Risiko zu bewerten.

IT-Sicherheitserfordernisse werden bei allen Projekten frühzeitig berücksichtigt (z. B. bei Planung eines neuen Netzes, Neuanschaffungen von IT-Systemen und Anwendungen, Outsourcing- und Dienstleistungsverträgen). IT-Sicherheitsaspekte werden zu Beginn eines Projektes im Projektplan (z. B. bei der Anschaffung neuer Software oder bei der Planung von Geschäftsprozessen) berücksichtigt. Neue Techniken werden nicht unkritisch eingesetzt (Checkliste). Klare Unterstützung der IT-Sicherheitsziele durch die Leitungsebene.

Sollten die IT-Sicherheitsaspekte nicht erreichbar sein, so werden evtl. Abstriche beim Komfort gemacht oder es wird auf bestimmte Funktionalitäten verzichtet.

Alternative Lösungsansätze mit zunächst bescheidenerer Zielsetzung werden immer in Erwägung gezogen.

Die Umsetzung wird ggf. in mehreren kleineren Schritten realisiert.

Bei der Umsetzung von Sicherheitszielen werden entspr. Handlungspläne erstellt, die die Sicherheitsziele priorisieren und die Umsetzung der beschlossenen IT-Sicherheitsmaßnahmen regeln.

Bei allen IT-Sicherheitsmaßnahmen ist festgelegt, ob sie einmalig oder in regelmäßigen Intervallen ausgeführt werden müssen (z. B. Update des Virenscanners).

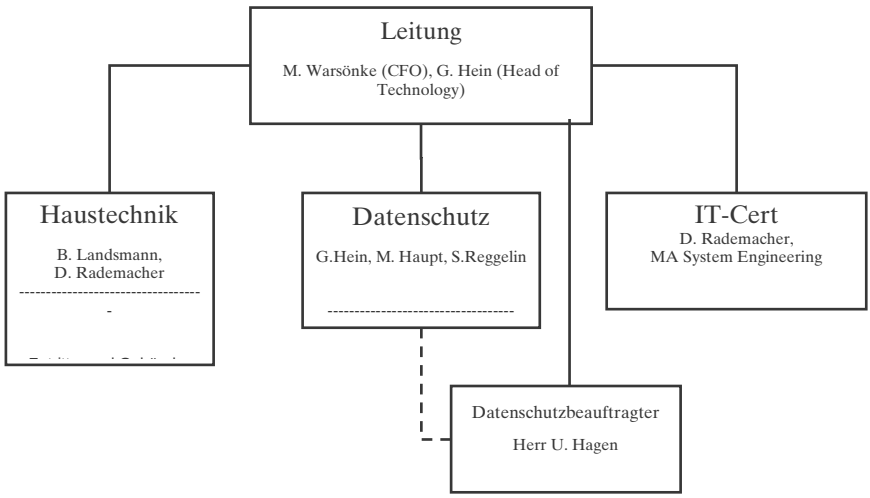
Die Wirksamkeit von IT-Sicherheitsmaßnahmen wird regelmäßig überprüft.

Organisation

In diesem Baustein werden die für die IT-Sicherheit grundlegend notwendigen organisatorischen Regelungen angeführt. Beispiele sind Festlegung der Verantwortlichkeiten, Datenträgerverwaltung und Regelungen zum Passwortgebrauch. Sie sind für jedes IT-System umgesetzt.

Sicherheits-Management Gremium

Gremium für das Sicherheits-Management



- Für alle IT-Sicherheitsmaßnahmen sind Zuständigkeiten und Verantwortlichkeiten festgelegt.
- Es gibt geeignete Vertretungsregelungen für Verantwortliche und die Vertreter sind mit ihren Aufgaben vertraut.
- Die wichtigsten Passwörter sind für Notfälle sicher hinterlegt.
- Die bestehende Richtlinien und Zuständigkeiten sind allen Zielpersonen bekannt.

Geeignete Regelungen zu jedem vorhandenen Sicherheitsziel und jeder zugehörigen Maßnahme

- „IT-Sicherheit im Unternehmen ist ein dauerhafter Prozess."
- Die meisten mit IT-Sicherheit assoziierten Aufgaben werden regelmäßig wiederholt und neu durchlaufen werden.
- Jede identifizierte Maßnahme wird dahingehend untersucht, ob sie nur ein einziges Mal oder regelmäßig ausgeführt werden muss (Beispiel: regelmäßiges Update des Virenscanners).

Organisatorische Maßnahmen

Handlungsplan mit klaren Prioritäten der Sicherheitsziele und -maßnahmen

- Eine geeignete Priorisierung der identifizierten Sicherheitsziele und -maßnahmen wird unter Abwägung des Kosten-Nutzen-Verhältnisses durchgeführt.

Besonders umständliche Sicherheitsanforderungen werden vermieden

- Es gibt i.d.R. nur Sicherheitsvorgaben, deren Einhaltung praktikabel ist
- Technische und organisatorische Infrastruktur wird bereitgestellt. Ggf. werden die technischen Anforderungen eher etwas herunterzuschrauben und dafür strenger auf deren Einhaltung geachtet.
- Alle Maßnahmen, die besonders tief in die gewohnte Arbeitsweise eingreifen, werden mit betroffenen Anwendern vorher besprochen.

Vorhandene Arbeitsabläufe und Sicherheitsrichtlinien werden regelmäßig hinsichtlich Zweckmäßigkeit und Effizienz überprüft

- Ständige Optimierung bestehender Prozesse und Richtlinien zur Abwehr von drei Hauptgefahren:
  - Prozesse und Richtlinien sind veraltet,
  - Prozesse und Richtlinien sind unvollständig oder
  - Prozesse und Richtlinien sind nicht praktikabel.
- Die ausführenden Personen bewerten persönlich die Arbeitsabläufe.
- Sind einzelne Maßnahmen als nicht zweckmäßig eingestuft worden, so wird gemeinsam nach Ursachen und Verbesserungspotentialgesucht werden.

Vorhandene Schutzmechanismen werden genutzt

- Die vom Hersteller implementierten Sicherheitsfunktionen und -mechanismen werden analysiert, verstanden und eingesetzt, bevor existierende Sicherheitsanforderungen nicht oder nur auf Umwegen umgesetzt werden.

Sicherheitsrichtlinien und -anforderungen werden beachtet

- Sicherheitsrichtlinien werden beachtet.
- Sicherheitsfunktionen und -programme werden entsprechend ihrer Möglichkeiten genutzt.

Am Arbeitsplatz sind keine sensitiven Informationen frei zugänglich

- Vertrauliche Akten werden bei Verlassen des Arbeitsplatzes im Schrank oder Safe verschlossen.
- Wird im Arbeitsvertrag
- Datenträger wie Bänder, Disketten und CD-ROMs sind nicht frei zugänglich, wenn sich vertrauliches Material darauf befindet. Sie werden sachgerecht entsorgt, um unbefugtes Rekonstruieren zu verhindern.
- Vertrauliche Ausdrucke werden mit einem Datenvernichter und nicht im normalen Papierkorb entsorgt. Datenträger wie Festplatten oder CD-ROMs werden vor der Entsorgung sicher gelöscht oder zerstört.

Bei Wartungs- und Reparaturarbeiten sind besondere Vorsichtsmaßnahmen zu beachten

- Servicetechniker arbeiten nie allein ohne Aufsicht an IT-Systemen oder TK-Anlagen.
- Auf Datenträgern, die das Haus verlassen, werden vorher alle Daten sorgfältig gelöscht.

Mitarbeiter werden regelmäßig geschult

- Es werden regelmäßig Maßnahmen ergriffen, um bei allen Beteiligten das Sicherheitsbewusstsein zu erhöhen. Z.B.: durch interne Vorträge, Schulungen, Newsletter, E-Mails, etc.
- Administratoren und IT-Sicherheitsverantwortliche nehmen an regelmäßigen Weiterbildungen teil.
- Entsprechende Fachliteratur ergänzt die Weiterbildungsmaßnahmen

Zugriff auf externes Fachwissen

- Sollte nicht für alle IT-Sicherheitsaspekte ist das notwendige Fachwissen in der eigenen Organisation vorhanden sein, wird Hilfe von externen Partnern in Anspruch genommen.

Für alle bestehenden Sicherheitsvorgaben sind Kontrollmechanismen vorhanden

- Für jede bestehende Sicherheitsvorgabe wird überlegt, wie deren Einhaltung kontrolliert werden kann. Die Kontrolle erfolgt durch technische Prüfwerkzeuge oder durch Auditoren bzw. Revisoren, durch Auswertung vorhandener Protokollierungsdaten, anhand von Stichproben durch Vorgesetzte etc.

- Abarbeitung geeigneter Checklisten.

Konsequenzen für Sicherheitsverstöße sind festgelegt und veröffentlicht

- Unternehmensweite INTERNET UND E-MAIL-RICHTLINIE von den Mitarbeitern zugestimmt

- Die (absichtliche oder versehentliche) Missachtung von Sicherheitsvorgaben zieht Konsequenzen nach sich.

- In der organisationseigenen Sicherheitsrichtlinie ist dargestellt, mit welchen Folgen im Ernstfall zu rechnen ist.

Erkannte Sicherheitsverstöße werden sanktioniert

- Im Bedarfsfall wird auf Sicherheitsverstöße angemessen reagiert. Die Tatsache, dass Verstöße geahndet werden, wird allen anderen kommuniziert, soweit die jeweilige Situation dies erlaubt.

Anlagen:

- Internet- und Email-Richtlinie als Anlage zum Arbeitsvertrag
- Computer-Richtlinie als Anlage zum Arbeitsvertrag
- Protokolle zu den regelmäßigen Sicherheits-Management-Meetings

Personal

Der Baustein „Personal“ beschreibt die Maßnahmen im Personalbereich, die für IT-Sicherheit zu beachten sind. Beispiele sind Vertretungsregelun-

gen, Schulungsmaßnahmen und geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern. Sie sind unabhängig von der Art der eingesetzten IT-Systems dargestellt.

Übersicht:

- Es gibt Checklisten, was beim Eintritt neuer Mitarbeiter und beim Austritt von Mitarbeitern zu beachten ist (Berechtigungen, Schlüssel, Unterweisung etc.)
  Prozessbeschreibung: Prozesse sind dokumentiert, Checklisten
- Die Mitarbeiter sind ausreichend geschult.

Maßnahmen:

Zuständigkeiten sind festgelegt

- Für jede identifizierte Aufgabe ist festgelegt, wer für die Durchführung verantwortlich ist.
- Für alle allgemein formulierten Sicherheitsrichtlinien ist genau dargelegt, für welchen Personenkreis diese verbindlich sind.
- Jeder Verantwortliche hat einen Stellvertreter.
  - Der Vertreter ist in der Lage, seine Aufgaben wahrzunehmen.
  - Wurde in seine Aufgaben eingewiesen.
  - Notwendige Passwörter sind für den Notfall hinterlegt.
  - Dokumentationen sind verfügbar.

Bestehende Richtlinien und Zuständigkeiten sind bekannt gemacht worden

- Internet- und E-Mail-Richtlinie
- Es ist sichergestellt, dass alle Betroffenen die Unternehmensrichtlinien – in ihrer aktuellen Fassung – kennen.
- Alle Mitarbeiter kennen ihre internen und externen Ansprechpartner und deren Kompetenzen.
- Im Bedarfsfall ist wird die Kenntnisnahme wichtiger Richtlinien von den Mitarbeitern schriftlich bestätigt.

Anlagen:

- Nachweise über die Teilnahme der Mitarbeiter-Datenschutzschulungen in der Personalabteilung

Notfallvorsorge-Konzept

Hier das Notfallvorsorge-Konzept erläutert. Dieser Baustein wird angewendet, weil in der Schutzbedarfsfeststellung Komponenten identifiziert wurden, die einen hohen Schutzbedarf in Bezug auf Verfügbarkeit haben und größere IT-Systeme bzw. umfangreiche Netze betrieben werden.

Übersicht

- Es gibt einen Notfallplan mit Anweisungen und Kontaktadressen.
- Alle notwendigen Notfallsituationen werden behandelt.
- Jeder Mitarbeiter kennt den Notfallplan und ihm ist dieser gut zugänglich.

Schutz vor Katastrophen und Elementarschäden

Notfallchecklisten sind erstellt und jedem Mitarbeiter bekannt gemacht

Wenn ein Rechner streikt, der Drucker nicht mehr druckt, der Strom ausfällt, das Netz von einem Virus befallen wurde oder Daten versehentlich gelöscht wurden sind die entsprechenden Mitarbeiter in der Lage den Fehler zu beheben.

Denkbare Szenarien werden von den Verantwortlichen in regelmäßigen Abständen durchgespielt.

Alle wichtigen Daten werden regelmäßig gesichert

Alle relevanten Daten werden vom eingerichteten Backup erfasst.

Es wird regelmäßig verifiziert, dass das Backup auch tatsächlich funktioniert und die Daten wieder erfolgreich eingespielt werden können.

Die Backup-Medien werden an sicherem Ort, möglichst außerhalb des Unternehmens bzw. des Dienstgebäudes, aufbewahrt. Der Aufbewahrungsort ist zudem hinreichend gegen Elementarschäden wie Feuer, Wasser und Ähnliches geschützt.

IT-Systeme werden angemessen gegen Feuer, Überhitzung, Wasserschäden und Stromausfall geschützt

Besonders wichtige IT-Komponenten (Server, Sicherungsmedien, Router etc.) sind in ausreichend geschützten Räumen untergebracht werden. Zusätzlich sind sie an eine unterbrechungsfreie Stromversorgung mit Überspannungsschutz angeschlossen sein.

Maßnahmen zum Zutrittsschutz und zum Schutz vor Einbrechern werden umgesetzt

Es wird berücksichtigt, wo sich Besucher und Betriebsfremde in der Regel aufhalten und auf welche IT-Systeme sie dabei zugreifen können.

Besonders Server oder Rechner, mit denen auf sensitive Daten zugegriffen wird, sind so aufgestellt sein, dass Fremde sich nicht unbemerkt an ihnen zu schaffen machen können.

Der gesamte Bestand an Hard- und Software ist in einer Inventarliste erfasst

Die Inventarliste wird regelmäßig aktualisiert. Ebenfalls wird der Standort erfasst.

Notfallvorsorgekonzept

Das Notfallvorsorgekonzept behandelt die Begrenzung größerer Schäden durch zügige und effiziente Behandlung.

Inhalt:

- Aufrechterhaltung der Geschäftstätigkeit während des Ausfalls des IT-Systems mit dem Ziel die Betriebsfähigkeit innerhalb einer tolerierbaren Zeitspanne wiederherzustellen
- Was ist zu tun, sobald ein Notfall/Sicherheitsvorfall bemerkt wird?
- Verhaltensregeln bei Sicherheitsvorfällen
- Alarmierung im Notfall
- Eskalationsstrategie
- Wiederanlauf
- Eingeschränkter IT-Betrieb
- Ausweichmöglichkeiten

- Aufrechterhaltung geschäftskritischer Prozesse
- Ausweich-IT-Systeme
- Ausweicharbeitsplätze
- manuelle Datenübertragung

Anlagen:

- Notfallvorsorgekonzept in Bearbeitung

Datensicherungskonzept

Dieser Baustein stellt dar, wie das Datensicherungskonzept aufgebaut ist. Dieser Baustein ist insbesondere für größere IT-Systeme oder IT-Systeme mit großem Datenbestand wichtig.

Übersicht:

- Es gibt eine Backupstrategie
- Es ist festgelegt, welche Daten wie lange gesichert werden.
- Die Sicherung bezieht auch tragbare Computer und nicht vernetzte Systeme mit ein.
- Die Sicherungsbänder werden regelmäßig kontrolliert.
- Die Sicherungs- und Rücksicherungsverfahren sind dokumentiert.

Datensicherungskonzept

Minderung der Folgen der speziellen Bedrohung

- des Verlusts,
- der Verfügbarkeit und
- der Integrität von Daten und IT-Systemen,
- bspw. resultierend aus
  - einem Computer-Virenbefall
  - einem Notfall

- einem Hardwaredefekt

Inhalt:

- Allgemeine Regelungen
- Regelung der Verantwortlichkeiten
- Verpflichtung der Benutzer auf Datensicherung

- Datensicherungspläne
  - Sicherung von Anwendungsdaten
  - Sicherung von Systemdaten
  - Sicherung von Protokolldaten
  - Sicherung von Software
- Rekonstruktion

Anlagen:

- Datensicherungskonzept für S-Box-Dokumentation in der IT-Systemtechnik

Datenschutz

Die Rahmenbedingungen für einen praxisgerechten Datenschutz und die Verbindung zur IT-Sicherheit über den IT-Grundschutz werden in diesem Baustein dargestellt.

Übersicht:

- Allen Systembenutzern sind Rollen und Profile zugeordnet.
- Es ist geregelt, auf welche Datenbestände jeder Mitarbeiter zugreifen darf.
- Es gibt verschiedene Rollen und Profile für Administratoren.
- Es ist bekannt und geregelt, welche Privilegien und Rechte Programme haben.

- Es werden sicherheitsrelevante Standardeinstellungen von Programmen und IT-Systemen geeignet angepasst. (Ausnahme für Druckerwartung: Admin-Passwörter bleiben auf Default).
- Nicht benötigte sicherheitsrelevante Programme und Funktionen werden konsequent deinstalliert bzw. deaktiviert.
- Vertrauliche Informationen und Datenträger werden sorgfältig aufbewahrt
- Vertrauliche Informationen werden vor Wartungs- oder Reparaturarbeiten von Datenträgern oder IT-Systemen gelöscht
- Mitarbeiter werden regelmäßig in sicherheitsrelevanten Themen geschult
- Es gibt Maßnahmen zur Erhöhung des Sicherheitsbewusstseins der Mitarbeiter
- Bestehende Sicherheitsvorgaben werden kontrolliert und Verstöße geahndet

Datenschutzmaßnahmen im Unternehmen:

Allen Systembenutzern sind Rollen und Profile zugeordnet

- Zugriffsberechtigungen für einzelne Personen oder Personengruppen sind mittels passender Berechtigungsprofile definiert.
- Jeder Benutzer (ebenso wie jeder Administrator) ist einer oder mehreren zulässigen Rollen zugeordnet, die er während seiner Arbeit annehmen kann.

Administratorrechte sind auf das erforderliche Maß eingeschränkt

- Maßnahmen zur Verringerung des Risikos einer erfolgreichen Übernahme der Administratorrolle durch unbefugte Dritte:
  - Es wird zwischen unterschiedlichen administrativen Aufgaben differenziert. Je nach administrativer Rolle kann ein Administrator nur bestimmte Aufgaben durchführen.
  - Es gibt einen gesonderten Administrator, der die Auswertung von Protokollierungsdaten vornimmt und die Aufgaben der anderen Administratoren überwachen kann.

Programmprivilegien sind begrenzt

- Ausführbare Programme verfügen – analog zu Anwendern – über bestimmte Zugriffsrechte und Systemprivilegien.
- Auch Programme sind nur mit den Berechtigungen ausgestattet sein, die sie für ein fehlerfreies Funktionieren benötigen.

Die Standardeinstellungen gemäß Auslieferungszustand werden bei neuen Systemen angepasst

- Standardpasswörter und Standard-Benutzer-Accounts sind deaktiviert. (Ausnahme für Druckerwartung: Admin-Passwörter bleiben auf Default)
- Ein neu installiertes und noch nicht an die eigenen (Sicherheits-) Bedürfnisse angepasstes System wird nie im produktiven Betrieb genutzt.
- Betriebssysteme besonders exponierter Rechner sowie wichtige Server werden gehärtet. D.b. die Entfernung aller Softwarebestandteile und Funktionen, die zur Erfüllung der vorgesehenen Aufgabe durch das Programm nicht zwingend notwendig sind.
- Alle unnötigen Anwendungsprogramme werden entfernt.

Zum Schutz von Netzen werden Firewalls verwendet

- Kein Computer, der geschäftsmäßig genutzt wird, ist ohne Schutz durch eine geeignete Firewall mit dem Internet verbunden.
- Teilnetze sind gegen benachbarte Netze abgesichert.

Alle Firewalls genügen den Mindestanforderungen

- Zum Schutz des internen Netzes gegen benachbarte, weniger vertrauenswürdige Netze wird ein geeigneter Firewalltyp eingesetzt.
- Ein mehrstufiges Firewallkonzept, bei dem zusätzliche Filterelemente (beispielsweise Router) vor- und nachgeschaltet werden, ist im Einsatz.
- Es wird regelmäßig geprüft ob die bestehenden Filterregeln noch konsistent sind, ob sie vereinfacht werden können und ob sie noch hinreichend restriktiv sind.

- Es wird in bestimmten Zeitabständen überprüft, ob die bestehende Firewallkonzeption noch den bereits eingeführten oder in Kürze zu erwartenden Kommunikationsprotokollen aus Sicht der IT-Sicherheit gewachsen ist.

Nach außen angebotene Daten werden auf das erforderliche Mindestmaß beschränkt

- Vertrauliche Daten werden durch zuverlässige Authentisierungs- und Autorisierungsmechanismen geschützt.

- Es wird regelmäßig geprüft, welche schutzbedürftige Daten außerhalb des eigenen, gut geschützten Netzes bereitgestellt und verarbeitet werden müssen.

Nach außen angebotene Dienste und Programmfunktionalität werden auf das erforderliche Mindestmaß beschränkt.

- Bei allen Funktionen, Serverdiensten und offenen Kommunikationsports, die nach außen angeboten werden, wird sorgfältig geprüft, ob dies wirklich erforderlich ist.

- Bei bestehenden Installationen wird regelmäßig überprüft, ob einzelne Dienste oder Funktionen aktiviert sein müssen.

Beim Umgang mit Web-Browsern werden riskante Aktionen unterbunden

- Im Web-Browser sind nur die aktiven Inhalte bzw. Skriptsprachen und Multimedia-PlugIns zugelassen werden, die für die Arbeit wirklich unverzichtbar sind.

Bei E-Mail-Anhängen ist besondere Vorsicht notwendig

- Die Verwendung eines Virenscanners ist Pflicht!

- Das automatische Öffnen von E-Mail-Anhängen wird durch geeignete Konfiguration sowie durch Zusatzprogramme technisch verhindert.

Datenzugriffsmöglichkeiten sind auf das erforderliche Mindestmaß beschränkt

- „Need-to-Know Prinzip“:

  - Jeder Benutzer (und auch jeder Administrator) kann nur auf die Datenbestände zugreifen und die Programme ausführen, die er für seine tägliche Arbeit auch wirklich benötigt.

- Informationen anderer Abteilungen sind nicht ohne weiteres von abteilungsfremden Mitarbeitern einsehbar, sofern sie diese Informationen nicht für ihre Arbeit benötigen.

- Anwendungsprogramme – insbesondere Programme für die Systemadministration – stehen nur den Mitarbeitern zur Verfügung, die diese wirklich brauchen.

- Erforderliche Berechtigungen werden in passenden Berechtigungsprofilen zusammengefasst.

- In regelmäßigen Abständen wird überprüft, ob die von einer Person verfügbaren Zugriffsrechte noch deren Tätigkeitsprofil entsprechen oder ob Einschränkungen zweckmäßig sind.

- Das eigene Netz wird regelmäßig mit passenden Tools untersucht.

- Ein geeigneter Prozess existiert, um Berechtigungen bei Einstellung/Ausscheiden von Mitarbeitern geeignet einzuräumen bzw. zu widerrufen.

Anlagen:

- BDSG §9 Technische und organisatorische Maßnahmen bei Proximity

- IT-Systeme (Übersicht für die Schutzbedarfsfeststellung)

- IT-Anwendungen (Übersicht für die Schutzbedarfsfeststellung)

- Netzplan

Computer-Virenschutzkonzept

Ziel des Computer-Virenschutzkonzeptes ist es, ein geeignetes Maßnahmenbündel zusammenzustellen, bei dessen Einsatz das Auftreten von Computer-Viren auf den in einer Organisation eingesetzten IT-Systemen verhindert bzw. möglichst früh erkannt wird, um Gegenmaßnahmen vornehmen zu können und mögliche Schäden zu minimieren.

Übersicht

- Aktuelle Virenschutzprogramme sind unverzichtbar.
- Es werden flächendeckend Virenschutzprogramme eingesetzt.
- Vorhandene Schutzmechanismen in Anwendungen und Programmen werden genutzt.
- E-Mails und jegliche Kommunikation über das Internet werden permanent zentral auf Viren untersucht. Zusätzlich ist jeder Computer mit einem lokalen Virenscanner ausgestattet, der permanent im Hintergrund läuft.

Computer-Virenschutz-Konzept

Gefährdung durch Computer-Viren-Infektion

- Verfügbarkeit von Daten bis hin ganzer Systeme
- Integrität der Daten und Systeme
- Vertraulichkeit der sensitiven Daten
- unterschiedliche Infektionswege
  - E-Mail (insb. durch die Attachments/Anhänge)
  - Internet (insb. durch aktive Inhalte und Sicherheitslücken)
  - internes Netz
  - (Vernetzung bis hin zu VPN ermöglicht Verbreitung)
  - Wechseldatenträger

Charakter einer Rahmenrichtlinie aufgrund

- ständiger Veränderung des Umfelds
- z. T. stark differenzierender Maßnahmen bei verschiedenen Betriebs- und anderen IT-Systemen

Begegnung der speziellen Bedrohungen eines Computer-Viren-Befalls

- Minimierung des Risikos eines Computer-Viren-Befalls
- Minderung der möglichen Folgen eines Computer-Viren-Befalls

steigende Gefährdung durch Computer-Viren-Angriffe

_ Einsatz des Konzepts in allen Größenklassen

Inhalt:

Computer-Viren-Verantwortlicher

Verhaltensregeln zur Vorbeugung

Verhaltensregeln bei Auftreten eines Computer-Virus

Anzeichen für einen Computer-Viren-Befall

Verhaltensregeln für den IT-Benutzer

Verhaltensregeln für den Computer-Viren-Verantwortlichen

Anlagen:

- Richtlinie für Virenschutz bei der internen EDV

Kryptokonzept

Dieser Baustein beschreibt die Vorgehensweise, wie in einer heterogenen Umgebung sowohl die lokal gespeicherten Daten als auch die zu übertragenen Daten wirkungsvoll durch kryptographische Verfahren und Techniken geschützt werden.

Verwendung von Sicherheitsmechanismen: Umgang mit Passwörtern und Verschlüsselung

Sicherheitsmechanismen sind sorgfältig ausgesucht

Es werden ausschließlich standardisierte, anerkannte Sicherheitsalgorithmen eingesetzt.

Die vorhandenen Schutzmechanismen werden in Abstimmung mit der Schutzstufe betrieben.

Es werden gut gewählte (sichere) Passwörter eingesetzt

Passwörtermüssen bestimmten Qualitätsanforderungen genügen:

- Es sollte länger als sieben Zeichen sein
- Nicht in Wörterbüchern vorkommen

- nicht aus Namen bestehen (insbesondere nicht von „Lieblingshelden“ aus Literatur und Film) und auch Sonderzeichen oder Ziffern enthalten.
- Im letztgenannten Fall sollten allzu gängige Varianten vermieden werden, wie beispielsweise Anhängen einfacher Ziffern am Ende des Passwortes oder eines der üblichen Sonderzeichen „$, !, ?, #“ am Anfang oder Ende eines ansonsten simplen Passwortes.
- Jedes Passwort muss in regelmäßigen Zeitabständen geändert werden.

Voreingestellte oder leere Passwörter werden geändert

- Bei neu installierten Produkten in IT-Systemen und modernen TK-Anlagen werden Accounts mit neuen Passwörtern versehen.

Anlagen:

- Einsatzmöglichkeiten von Verschlüsselungssoftware bei der IT-Systemtechnik

Behandlung von Sicherheitsvorfällen

Um die IT-Sicherheit im laufenden Betrieb aufrecht zu erhalten, ist es notwendig, die Behandlung von Sicherheitsvorfällen (Incident Handling) konzipiert und eingeübt zu haben. Als Sicherheitsvorfall wird dabei ein Ereignis bezeichnet, das Auswirkungen nach sich ziehen kann, die einen großen Schaden anrichten können. Um Schäden zu verhüten bzw. zu begrenzen, verläuft die Behandlung der Sicherheitsvorfälle zügig und effizient. Dieser Baustein wird angewendet, weil in der Schutzbedarfsfeststellung Komponenten identifiziert wurden, die einen hohen Schutzbedarf in Bezug auf einen der drei Grundwerte haben, und da der Ausfall des gesamten IT-Verbunds einen Schaden in den Kategorien hoch oder sehr hoch zur Folge hat.

Vernetzung und Internet-Anbindung

- Es werden Firewalls eingesetzt.
- Konfiguration und Funktionsfähigkeit der Firewalls werden regelmäßig kritisch überprüft und kontrolliert.

Infrastruktursicherheit

- Es besteht ein angemessener Schutz der IT-Systeme gegen Feuer, Überhitzung, Wasserschäden, Überspannung und Stromausfall
- Der Zutritt zu wichtigen IT-Systemen und Räumen ist geregelt. Besucher, Handwerker, Servicekräfte etc. werden begleitet bzw. beaufsichtigt.
- Es besteht ein ausreichender Schutz vor Einbrechern.
- Der Bestand an Hard- und Software ist in einer Inventarliste erfasst.

Anlagen :

- s. Notfallvorsorgekonzept

Hard- und Software-Management

Ziel des Bausteins „Hard- und Software-Management“ ist es, einen ordnungsgemäßen IT-Betrieb im Hinblick auf Management bzw. Organisation sicherzustellen. Hierzu enthält der Baustein schwerpunktmäßig Empfehlungen zu Regelungen und Abläufen, die sich spezifisch auf informationstechnische Hardware- oder Software-Komponenten beziehen.

- Handbücher und Produktdokumentationen werden frühzeitig gelesen.
- Es werden ausführliche Installations- und Systemdokumentationen erstellt und regelmäßig aktualisiert

Vernetzung und Internet-Anbindung

- Es gibt es ein Konzept, welche Daten nach außen angeboten werden müssen.
- Alle unnötigen Dienste und Programmfunktionen werden deaktiviert.
- Web-Browser und E-Mail-Programme sind sicher konfiguriert.
- Es ist festgelegt, wie mit gefährlichen Zusatzprogrammen (PlugIns) und aktiven Inhalten umgegangen wird.

Sicherheits-Updates werden regelmäßig eingespielt

Liste der relevanten Sicherheits-Updates:

- Betriebssysteme
- Virenschutzprogramme.
- E-Mail-Programme
- Web-Browser

Von den Verantwortlichen werden in regelmäßigen Abständen ausführliche Recherchen zu den Sicherheitseigenschaften der verwendeten Software durchgeführt

- Eine regelmäßige Informationsbeschaffung über neu aufgedeckte Schwachstellen und Hilfsmittel zu deren Beseitigung wird durchgeführt.
- Die Systemverantwortlichen bringen in regelmäßigen Abständen die Zeit für entsprechende Suchen im Internet und für den Austausch mit Fachkollegen auf.
- Es sind Auswahlkriterien festgelegt, die definieren, welche Updates mit wie viel Zeitverzug installiert werden können bzw. müssen.

Aktionspläne zum Einspielen erforderlicher Sicherheits-Updates liegen vor

- Das Einspielen von Updates erfordert sehr viel Disziplin und ist deshalb von vornherein als Prozess verankert.
- Virenscanner können schnellstmöglich aktualisiert werden.

Softwareänderungen werden getestet werden

Jede Softwareänderung an Produktivsystemen wird zuvor ausgiebig in einer Testumgebung überprüft.

Passwörter und Verschlüsselung

- Programme und Anwendungen bieten Sicherheitsmechanismen wie Passwortschutz oder Verschlüsselung. Die Sicherheitsmechanismen sind aktiviert.
- Voreingestellte oder leere Passwörter werden geändert.

- Alle Mitarbeiter sind in der Wahl sicherer Passwörter geschult.
- Arbeitsplatzrechner werden bei Verlassen mit Bildschirmschoner und Kennwort gesichert.
- Vertrauliche Daten und besonders gefährdete Systeme wie Notebooks werden ausreichend durch Verschlüsselung oder andere Maßnahmen geschützt.

Die IT-Sicherheit wird regelmäßig überprüft

- Das Niveau der IT-Sicherheit wird regelmäßig bewertet und kontrolliert.
- Wenn ein ausreichendes Budget zur Verfügung steht, wird einmal pro Jahr ein unabhängiger Experte mit der Überprüfung von besonders kritischen Bereichen der IT beauftragt.
  - Gibt es neue Sicherheitsstandards oder
  - neue, wichtige Techniken?
  - Haben sich die Erwartungen von Kunden und Geschäftspartnern geändert?

Handbücher und Produktdokumentationen werden frühzeitig gelesen

- Warnhinweise des Herstellers werden berücksichtigt.

Ausführliche Installations- und Systemdokumentationen ist erstellt und wird regelmäßig aktualisiert

- Alle Arbeitsschritte vor, während und nach einer Installation sind schriftlich dokumentiert.
- Die Systemdokumentation kann auch von Dritten (beispielsweise im Sinne eines „Ersatzadministrators“ oder einer Urlaubsvertretung) nachvollzogen und verstanden werden.

Unbefugte Veränderungen am System werden somit schneller identifiziert.

Arbeitsplatzrechner sollten bei Verlassen mit Bildschirmschoner und Kennwort gesichert werden

- Bildschirmschoner sollten benutzt werden, wenn unbefugte Dritte bei vorübergehender Abwesenheit des rechtmäßigen Benutzers Zugang zu dessen PC erlangen könnten.

- Ein häufig angewandter Zeitpunkt ist fünf Minuten nach der letzten Benutzereingabe.

Sensitive Daten und Systeme werden geschützt

Der Einsatz einer Verschlüsselungssoftware für vertrauliche Dateien wird gem. Sicherheitsanalyse erwogen. Notebooks werden ggf. komplett verschlüsselt

Anlagen:

- Richtlinien für Proximity Systemtechnik und interner EDV müssen erstellt werden

Outsourcing

Der Baustein Outsourcing beschreibt die IT-Sicherheitsmaßnahmen, die bei den zu externen Dienstleistern ausgelagerten Arbeits- oder Geschäftsprozessen der Organisation zu beachten sind. Outsourcing kann sowohl Nutzung und Betrieb von Hardware und Software, aber auch Dienstleistungen betreffen.

Anlagen:

- IT-Prozesse zwischen Proximity und der BSG
- IT-Anwendungen (Übersicht für die Schutzbedarfsfeststellung)