Aktuelle Förderbekanntmachung

Bekanntmachung des Ministeriums für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen (MWIKE) zur Durchführung des Förderprogramms

„Mittelstand Innovativ & Digital“ (MID)-Digitale Sicherheit

vom 5. Oktober 2022

1. Zuwendungszweck und Rechtsgrundlagen

1.1 Zuwendungszweck

Mit dem Programm Mittelstand Innovativ & Digital (MID) stärkt das Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen (MWIKE) branchenübergreifend kleine und mittlere Unternehmen (KMU) darin, die Innovationskraft ihrer Betriebe zu stärken und ihre Produkte, Dienstleistungen und Prozesse digital und sicher weiterzuentwickeln, um so auch in Zukunft einer der wirtschaftlichen Motoren des Landes zu sein.

Während es die drei Varianten der Gutscheinförderung MID-Digitalisierung, MID-Analyse und MID-Innovation Unternehmerinnen und Unternehmern ermöglichen, projektbezogen externe Unterstützung für speziell auf den Betrieb zugeschnittene Beratungs-, Entwicklungs- und Umsetzungsdienstleistungen hinzuzuziehen, können kleine Unternehmen mithilfe eines MID-Assistenten oder einer MID-Assistentin eine Hochschulabsolventin oder einen Hochschulabsolventen projektbezogen einstellen und so einen konkreten Wissenstransfer von Hochschulen in den Betrieb einbringen.

Das Teilprogramm MID-Invest unterstützt kleine und mittlere Unternehmen darin, Investitionen in spezifische technologiebasierte Hardware und Software zu tätigen.

Durch die fortschreitende Digitalisierung in Unternehmen und Gesellschaft entstehen immer neue IT-Anwendungen und Services. Damit gehen unweigerlich potentielle Sicherheitslücken einher, die wiederum cyberkriminelle Straftaten befördern können. Mit Hilfe des Teilprogramms MID-Digitale Sicherheit können kleine und mittlere Unternehmen durch technische Vorkehrungen und Anwendungen sowie durch die Sensibilisierung der Mitarbeitenden anwendungsspezifisch ihre Cyber-Resilienz erhöhen.

1.2 Rechtsgrundlagen

1.2.1 Das Land gewährt auf Antrag Zuwendungen nach Maßgabe der §§ 23, 44 der Landeshaushaltsordnung des Landes Nordrhein-Westfalen (LHO NRW) in der Fassung der Bekanntmachung vom 26. April 1999 (GV. NRW. S. 158) in der jeweils geltenden Fassung und den hierzu erlassenen Allgemeinen Verwaltungsvorschriften vom 10. Juni 2020 (MBl. NRW. S. 303-316).

1.2.2 Bestandteil des Zuwendungsbescheids auf Ausgabenbasis sind die Allgemeinen Nebenbestimmungen für Zuwendungen zur Projektförderung (ANBest-P) in der jeweils aktuell gültigen Fassung.

1.2.3 Die Zuwendung erfolgt als De-minimis-Beihilfe i. S. der Verordnung (EU) Nr. 1407/2013 vom 18. Dezember 2013 über die Anwendung der Artikel 107 und 108 des Vertrags über die Arbeitsweise der Europäischen Union auf De-minimis-Beihilfen (im Folgenden: De-minimis-Verordnung[1]). Die in der De-minimis-Verordnung genannten Voraussetzungen müssen für die Gewährung der Zuwendung gegeben sein. Der Gesamtbetrag der einem Unternehmen von einem Mitgliedstaat gewährten De-minimis-Beihilfen darf innerhalb eines fließenden Zeitraumes von drei Steuerjahren den Betrag von 200.000 EUR nicht überschreiten.

[1] Verordnung (EU) Nummer 1407/2013 der Kommission vom 18. Dezember 2013 über die Anwendung der Artikel 107 und 108 des Vertrags über die Arbeitsweise der Europäischen Union auf De-minimis-Beihilfen (ABl. L 352 vom 24. Dezember 2013, S. 1) in der Fassung der Verordnung (EU) 2020/972 der Kommission vom 2. Juli 2020 (ABl. L 215 vom 7. Juli 2020, S. 3).

1.2.4 Die Bestimmung des KMU-Status erfolgt gemäß der Empfehlung der Europäischen Kommission 2003/361/EG vom 06.05.2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (im Folgenden: KMU-Empfehlung)[2].

1.2.5 Ein Rechtsanspruch auf Förderung besteht nicht. Es handelt sich um eine freiwillige Leistung des Landes Nordrhein-Westfalen, über welche die Bewilligungsbehörde nach pflichtgemäßem Ermessen im Rahmen der verfügbaren Haushaltsmittel entscheidet. Für die beantragte Maßnahme dürfen keine weiteren öffentlichen Zuschüsse aus Mitteln des Landes, des Bundes oder der EU in Anspruch genommen werden (Ausschluss der Doppelförderung). Das gilt nicht für öffentliche Darlehen und Bürgschaften. Die Kumulierungsvorschriften der De-minimis-Verordnung sind zu beachten.

2. Gegenstand der Förderung

Gefördert wird die Umsetzung von spezifischen Maßnahmen zur Steigerung der digitalen Sicherheit in Kleinstunternehmen, kleinen und mittleren Unternehmen aller Branchen mit Sitz in Nordrhein-Westfalen. MID-Digitale Sicherheit fördert Maßnahmen in den drei sich ergänzenden Schwerpunkten A, B und C, die beliebig kombiniert werden können. Somit leistet MID-Digitale Sicherheit einen Anreiz zur Etablierung anwendungsspezifischer Sicherheitsstandards im Unternehmen, um Sicherheitsschwachstellen zu erkennen und Cyberangriffe abzuschirmen. Weiterführende Informationen zum Programmteil MID-Digitale Sicherheit finden Sie unter:

www.mittelstand-innovativ-digital.nrw/mid-digitale-sicherheit

MID-Digitale Sicherheit umfasst die folgenden drei Schwerpunktbereiche. Eine detaillierte Auflistung der förderfähigen Maßnahmen ist in Anlage A aufgeführt.

2.1 Schwerpunkt A: Analyse des IST-Zustandes in der Organisation

Grundvoraussetzung zur Steigerung der digitalen Sicherheit von Netzen und IT-Systemen in einem sich rasant ändernden virtuellen Umfeld ist eine präzise Risikoanalyse der zu schützenden IT-Infrastruktur.
Schwerpunkt A unterstützt dabei, den IST-Zustand der IT-Systeme zu definieren, die Gefährdung herauszuarbeiten, den Schutzbedarf zu bestimmen und darauf aufbauend das erforderliche Schutzniveau zu definieren.
Der Schwerpunkt bildet die Grundlage für die Planung und Umsetzung angemessener Maßnahmen zur Behebung/Reduktion von Schwachstellen.

Im Rahmen des Schwerpunktes sind ausschließlich IT-Dienstleistungen durch ein externes auftragnehmendes Unternehmen förderfähig.

[2] Empfehlung der Europäischen Kommission 2003/361/EG vom 06.05.2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (Amtsblatt der EU Nr. L 124/36 vom 20.05.2003).

2.2 Schwerpunkt B: Faktor Mensch - nutzerorientierte Maßnahmen

Ein weiterer elementarer und nicht zu vernachlässigender Schwerpunkt zur Steigerung der Cyber-Resilienz sind die Mitarbeitenden im Unternehmen bzw. der Faktor Mensch. Die aufwendigsten Sicherheitsvorkehrungen können ins Leere laufen, wenn diese im Arbeitsalltag nicht umgesetzt und angewendet werden.

Unsichere Passwörter oder die Preisgabe von sensiblen Zugangsdaten sind beispielsweise ebenfalls Wege für Cyber-Angriffe fernab von technischen Sicherheitslücken, die auch durch die besten Schutzprogramme nicht abwehrbar sind.

Daher sind die Mitarbeitenden – von den Nutzenden der Informationstechnik bis hin zur Administration, von der Arbeitsebene bis hin zur Leitungsebene - umfassend für Sicherheitsmaßnahmen zu sensibilisieren und zu schulen. Außerdem bietet der Schwerpunkt die Möglichkeit, Mitarbeitende im Bereich digitale Sicherheit gezielt fortzubilden.

2.3 Schwerpunkt C: Software für den IT-Basisschutz

Hierbei liegt der Fokus auf dem Erwerb von Antiviren-, Anti-Ransom- und DDoS-Schutz-Software bzw. entsprechender Lizenzen, deren Wartung/Updates sowie deren Einbindung.

2.4 Die Bewilligungsbehörde behält sich vor, weitere Maßnahmen/Ausgaben im Rahmen der Antragsprüfung von der Förderung auszuschließen, sofern diese nicht mit den Förderbestimmungen und Zielen des Programmes vereinbar sind.

3. Zuwendungsempfänger

3.1 Antragsberechtigt sind Unternehmen, die:

a) Im Sinne der KMU-Empfehlung (vgl. 1.2.4)

Kleinstunternehmen mit weniger als 10 Mitarbeitenden und einem Jahresumsatz oder einer Jahresbilanzsumme von höchstens 2 Mio. EUR,

oder

Kleine Unternehmen mit weniger als 50 Mitarbeitenden und einem Jahresumsatz oder einer Jahresbilanzsumme von höchstens 10 Mio. EUR

oder

Mittlere Unternehmen mit weniger als 250 Mitarbeitenden und entweder einem Jahresumsatz von höchstens 50 Mio. EUR oder einer Jahresbilanzsumme von höchstens 43 Mio. EUR sind.

b) ein „eigenständiges Unternehmen“ sind und nach der Ermittlungsmethode gemäß Artikel 6 des Anhangs der KMU-Empfehlung zusammen mit ihren „Partnerunternehmen“ bzw. „verbundenen Unternehmen“ die zuvor genannten Voraussetzungen (Anzahl Mitarbeitende, Jahresumsatz/Jahresbilanzsumme) nicht überschreiten.

c) ihren Sitz[3] am Tag der Antragstellung in Nordrhein-Westfalen haben

[3] Sitz entspricht der Geschäftsanschrift bspw. wie im Handelsregisterauszug oder auf der Gewerbeanmeldung angegeben.

d) zur Durchführung der Maßnahme nicht über die notwendige fachliche Expertise verfügen.

3.2 Ausgeschlossen von der Förderung sind:

a) Unternehmen, deren Geschäftsführung bzw. Anteilseignende Familienangehörige (z. B. Ehepartner, Lebenspartner, Geschwister) der Geschäftsführung bzw. Anteilseignende der beabsichtigten auftragnehmenden Unternehmen sind.

b) Unternehmen, deren Geschäftsführung bzw. Anteilseignende die gleichen natürlichen Personen wie die Geschäftsführung bzw. Anteilseignende des beabsichtigten auftragnehmenden Unternehmens sind.

c) Unternehmen, die bereits Anteile am auftragnehmenden Unternehmen halten bzw. bei denen das auftragnehmende Unternehmen Anteile am auftraggebenden Unternehmen hält. Im Falle einer Beteiligungsgesellschaft dürfen neben dieser auch deren Gesellschaftende nicht bereits Anteile am Unternehmen halten.

4. Zuwendungsvoraussetzungen

4.1 Die Wahl des auftragnehmenden Unternehmens erfolgt durch das auftraggebende Unternehmen nach wettbewerblichen Gesichtspunkten zu wirtschaftlichen Bedingungen. Das auftragnehmende Unternehmen muss in dem Themengebiet, welches es später im Rahmen des Projektes bearbeitet, einschlägige Referenzen/Kompetenzen aufweisen. Die Bewilligungsbehörde behält sich vor, dies im Rahmen der Antragsbewilligung zu prüfen.

4.2 Es werden alle auftragnehmenden Unternehmen mit Sitz in der Europäischen Union akzeptiert. Eine Zertifizierung ist nicht erforderlich.

4.3 Die Vergabe von Unteraufträgen im Zusammenhang mit der Leistungserbringung ist nicht zulässig. Die Bewilligungsbehörde behält sich vor, dies im Rahmen der Antragsbewilligung zu prüfen.

4.4 Das auftragnehmende Unternehmen kann nicht zugleich auftraggebendes Unternehmen in derselben Fördermaßnahme sein.

4.5 Das antragstellende Unternehmen muss in der Lage sein, den nicht geförderten, für die Tätigung der Maßnahme aber notwendigen Eigenanteil selbst oder von Dritten (ausgenommen sind zweckgebundene Zuwendungen im Sinne der §§ 23, 44 LHO NRW oder vergleichbarer Regelungen oder Aufträge im Sinne der Unterschwellenvergabeordnung oder vergleichbarer Regelungen anderer juristischer Personen des öffentlichen Rechts für das beantragte Projekt) aufzubringen.

4.6 Antragstellende Unternehmen, die sich am 31. Dezember 2019 bereits in Schwierigkeiten gemäß Art. 2 Abs. 18 der Allgemeinen Gruppenfreistellungsverordnung befanden, sind von der Förderung nach dieser Förderbekanntmachung ausgeschlossen, es sei denn sie waren in der Folge zumindest vorübergehend keine Unternehmen in Schwierigkeiten oder sind derzeit keine Unternehmen in Schwierigkeiten mehr.

Abweichend davon können Beihilfen für kleine Unternehmen (im Sinne des Anhangs I der Allgemeinen Gruppenfreistellungsverordnung) gewährt werden, die sich am 31. De-

zember 2019 bereits in Schwierigkeiten befanden, sofern diese Unternehmen nicht Gegenstand eines Insolvenzverfahrens nach nationalem Recht sind und sie weder Rettungsbeihilfen noch Umstrukturierungsbeihilfen erhalten haben.

4.7 Förderfähig sind nur Maßnahmen, die noch nicht begonnen wurden. Die Maßnahme gilt als begonnen, wenn bereits eine rechtsverbindliche Bestellung getätigt oder ein Auftrag/Vereinbarung zur Erbringung der Dienstleistung erteilt wurde.

4.8 In einem Zeitraum von zwei Jahren kann der Programmteil von einem Unternehmen nur einmal in Anspruch genommen werden. Maßgeblich für die Berechnung dieser Frist ist das Datum des letzten Mittelabrufs bzw. des jeweiligen Förderbausteines. Dies schließt verbundene Unternehmen und Partnerunternehmen mit ein (vgl. 1.2.4).

5. Art, Umfang und Höhe der Zuwendung

5.1 Die Zuwendung wird im Rahmen der Projektförderung in Form eines nicht rückzahlbaren Zuschusses als Anteilfinanzierung gewährt.

5.2 Als Bemessungsgrundlage für den Zuschuss werden die für die Umsetzung des Vorhabens erforderlichen Ausgaben im Angebot des Kooperationspartners zugrunde gelegt.

a) Die bewilligende Stelle behält es sich vor, Positionen des Angebotes, welche nicht zuwendungsfähig sind, ersatzlos zu streichen und anhand dieser korrigierten Summe die Zuwendung zu berechnen.

b) Es können nur Nettobeträge anerkannt werden, eine Förderung der Umsatzsteuer ist ausgeschlossen.

5.3 Der Durchführungszeitraum, also die maximale Bearbeitungsdauer, zur Umsetzung des Vorhabens beträgt wahlweise:

a) 6 Monate

b) 9 Monate

c) 12 Monate

Der Durchführungszeitraum muss bei der Beantragung festgelegt werden und dient der Berechnung aller weiteren Fristen.

5.4 Die maximale Zuwendungssumme beträgt 15.000 €.

5.5 Förderquoten und minimale Zuwendung (Bagatellgrenze) für MID-Digitale Sicherheit:

Unternehmensgröße*	**Förderquote MID-Digitale Sicherheit**	**Minimale Zuwendung MID-Digitale Sicherheit (Bagatellgrenze)**
Kleinstunternehmen	80 %	4.000,00 €
Kleine Unternehmen		
Mittlere Unternehmen	60 %	

*Vgl. 3.1 a) und b)

6. Verfahren

Das Verfahren bzw. der Antragsprozess ist nach einem „Windhundverfahren“ ausgelegt. Es stehen folglich eine pro Monat festgeschriebene Anzahl von Förderfällen zur Verfügung. Ist die maximale Anzahl erreicht, schließt das System und öffnet automatisch wieder zum ersten Tag des Folgemonats.

6.1 Förmliche Förderanträge müssen digital über das Förderportal MID-Digitale Sicherheit unter

www.mittelstand-innovativ-digital.nrw/antrag/mid-digitale-sicherheit

abgerufen und eingereicht werden.
Anträge und Dokumente können schriftlich oder gemäß der Verwaltungsvorschrift Nummer 14.1 zu § 44 LHO in Verbindung mit § 3 a Verwaltungsverfahrensgesetz für das Land Nord-rhein-Westfalen (VwVfG NRW) in der Fassung der Bekanntmachung vom 12. November 1999 (GV. NRW. S. 602) in der jeweils geltenden Fassung elektronisch übermittelt werden.

6.2 Antrag auf Förderung

6.2.1 Der Antrag muss die folgenden Angaben enthalten:

a) Name und Adresse des antragstellenden Unternehmens,

b) Beschreibung der Maßnahme,

c) Beschreibung des antragstellenden Unternehmens,

d) Tätigkeitsbeschreibung des auftragnehmenden Unternehmens

e) Angaben zum auftragnehmenden Unternehmen

f) Angaben zu De-minimis-Förderungen

6.2.2 Der Antrag muss folgende Unterlagen enthalten:

a) Abschließende Erklärung zur Antragstellung MID-Digitale Sicherheit

b) Ein Nachweis über die Geschäftstätigkeit (Kopie der Gewerbeanmeldung/des Handelsregisterauszuges (als GmbH, e.K., UG, AG, oHG, KG, GmbH & Co.KG ist zwingend der Handelsregisterauszug beizufügen), eine Bescheinigung des Finanzamtes (bei freiberuflich tätigen Personen)),[4]

c) Ein aktuelles, unverbindliches aber aussagekräftiges Angebot des auftragnehmenden Unternehmens. Es ist nur das Angebot eines auftragnehmenden Unternehmens förderfähig, mit Ausnahme von Nr. B3.

6.2.3 Nur vollständige Anträge können berücksichtigt werden.

[4] Für Kleingewerbe-Betriebe und Gesellschaften des bürgerlichen Rechts (GbR) ist der Eintrag freiwillig. Hier ist als Nachweis eine Gewerbeanmeldung ausreichend. Freiberufler/-innen reichen eine Bescheinigung in Steuersachen des zuständigen Finanzamtes, Steuerberater-/innen einen Nachweis über die Eintragung bei der Steuerberaterkammer und Ärzte/Ärztinnen oder Arztpraxen einen Nachweis über die Eintragung bei der Ärztekammer bzw. in das Partnerschaftsregister ein.

6.2.4 Die eingegangenen Anträge werden gemäß den formalen und inhaltlichen Anforderungen dieser Förderbekanntmachung bewertet.

6.2.5 Über eine Förderung entscheidet der Projektträger Jülich, Forschungszentrum Jülich GmbH, Wilhelm-Johnen-Straße, 52425 Jülich als Bewilligungsbehörde.

6.2.6 Förderanträge können fortlaufend eingereicht werden. Der Zuwendungsgeber behält sich vor, jederzeit einen Antragsstopp für das gesamte Programm MID oder einen spezifischen Programmteil unter

www.mittelstand-innovativ-digital.nrw

zu verkünden. Dies gilt insbesondere für den Fall, dass die verfügbaren Haushaltsmittel ausgeschöpft worden sind oder das monatliche Antragskontingent erreicht wurde. Anträge, die nach dem Zeitpunkt des Antragsstopps eingehen, können nicht mehr berücksichtigt werden.

6.2.7 Von der Anwendung der ANBest-P ausgenommen sind die Regelungen der Nummer 3. In den Zuwendungsbescheid sind die Vorgaben aus Nummer 7 und 8 dieser Förderbekanntmachung aufzunehmen.

6.3 Abruf von Fördergeldern

6.3.1 Nach Abschluss der Maßnahme, werden die Fördergelder innerhalb eines im Zuwendungsbescheid genannten Zeitraumes beim Projektträger Jülich durch Anforderung der Zuwendungsmittel abgerufen.

6.3.2 Die Bereitstellung der Fördergelder erfolgt nach dem Ausgabenerstattungsverfahren, d. h. das Unternehmen tritt zunächst in Vorleistung.

6.3.3 Die Erstattung erfolgt einmalig nach Abschluss der Maßnahme und Begleichung einer Schlussrechnung, es kann keine Zwischenrechnung bei dem Projektträger eingereicht werden.

6.3.4 Der Abruf von Fördergeldern soll in digitaler Form über das Förderportal erfolgen. Alternativ können auf Nachfrage auch die benötigten Antragsformulare außerhalb des Förderportals ausgestellt werden.

6.3.5 Zum Abruf der Fördergelder müssen der Bewilligungsbehörde folgende Angaben und Anlagen bereitgestellt werden:

a) Anforderung der Zuwendungsmittel,

b) Verwendungsnachweis

c) Eine Kopie der Rechnung des auftragnehmenden Unternehmens inkl. Angabe des Anschaffungszeitpunktes

d) Zahlungsnachweis/Buchungsbeleg (Kopie Kontoauszug)

e) Kurzer Sachbericht

6.4 Projektänderungen bedürfen der Rücksprache mit der Bewilligungsbehörde und einer entsprechenden Freigabe.

7. Projektmonitoring / Evaluation

7.1 Das zuwendungsempfangende Unternehmen ist zu einer engen Zusammenarbeit mit der Bewilligungsbehörde verpflichtet.

7.2 Der Zuwendungsgeber ist grundsätzlich berechtigt, über die Projekte folgende Angaben bekannt zu geben:

a) das Thema des Vorhabens,

b) das zuwendungsempfangende sowie das auftragnehmende Unternehmen,

c) die für die Durchführung des Vorhabens verantwortliche Person,

d) den Bewilligungszeitraum,

e) die Höhe der Zuwendung und der Eigenbeteiligung des zuwendungsempfangenden Unternehmens.

7.3 Für die Durchführung der Erfolgskontrolle und Evaluation auf Programmebene und für die Bewertung der Umsetzung des Förderprogramms sowie der mit den Förderprojekten erreichten Ergebnisse ist es erforderlich, dass der Zuwendungsgeber, der Projektträger bzw. die gegebenenfalls mit einer Evaluation beauftragten Institutionen während und nach der Laufzeit des Förderprogramms die notwendigen Daten und Informationen erhalten.

Zuwendungsempfangende Unternehmen haben daher projektbezogene Informationen, auch über den üblichen Inhalt eines Zwischen- und Verwendungsnachweises hinaus, sowie unternehmensbezogene Angaben, die bei der Antragstellung relevant waren oder allgemeiner Art sind, auf Nachfrage zur Verfügung zu stellen.

7.4 Der Zuwendungsgeber, der Projektträger bzw. die mit einer Evaluation beauftragten Institutionen sind verpflichtet, die Informationen vertraulich zu behandeln und ausschließlich zu dem bezeichneten Zweck zu verwenden.

8. Veröffentlichung der Projektergebnisse

8.1 Im Falle einer Öffentlichkeitsarbeit zu dem geförderten Vorhaben ist das zuwendungsempfangende Unternehmen dazu verpflichtet, durch die sichtbare Platzierung des MID-Logos auf der Firmenhomepage oder in entsprechenden Dokumenten auf die Förderung des Projekts hinzuweisen und den Projektträger darüber zu informieren. Dies gilt insbesondere für Veröffentlichungen (Broschüren, Faltblätter, Mitteilungsblätter) sowie Informationsveranstaltungen, Workshops, Symposien u. ä. im Zusammenhang mit dem Projekt. Das MID-Logo darf vom zuwendungsempfangenden Unternehmen nicht bearbeitet werden.

8.2 Für die entsprechende Öffentlichkeitsarbeit ist die folgende Formulierung zu verwenden:

Dieses Vorhaben wurde aus Mitteln des Förderprogramms Mittelstand Innovativ & Digital (MID) des Landes NRW gefördert.

Anlage A

Hierbei handelt es sich um eine beispielhafte Auflistung von förderfähigen Maßnahmen im Teilprogramm MID-Digitale Sicherheit in den drei Schwerpunkten A, B und C. Die einzelnen Maßnahmen sind beliebig kombinierbar:

Schwerpunkt A: Analyse des IST-Zustandes in der Organisation

A1. Analyse der zu schützenden Infrastruktur als Basis zur Durchführung und Planung weiterer Maßnahmen / Sicherheitsassessments

a) Analyse der bereits bestehenden IT-Schutzmaßnahmen

b) Durchführung einer herstellerneutralen Cyber-Sicherheitsberatung

c) Penetrationstests durch Simulation von externen Angriffen / interner Penetrationstest

d) Durchführung von Audits zur Digitalen Sicherheit

e) Aufnahme des IST-Zustands, Interne Schwachstellen-Überprüfungen durch IT-Dienstleistung im Sinne der unten aufgeführten Punkte

- Aufnahme des IST-Zustandes, durch Aufnahme der verschiedenen IT-Infrastrukturen
- Überblick und Überprüfung der aktuell verwendeten IT-Systeme / Informationssicherheits-Revisionen
- Überprüfung der Notwendigkeit der vorhandenen IT-Systeme
- IST-Zustand Netzstrukturaufnahme / Identifikation von Netzübergängen (bspw.: individuelle DSL-Zugänge, selbst eingerichtete VPN-Zugänge o.ä.)

A2. Behebung der erkannten Schwachstellen und Sicherheitslücken durch Verbesserung der eingesetzten IT-Systeme

a) Dienstleistungen zur Anpassung/Neustrukturierung der Netzumgebung zur Erhöhung der Schutzwirkung z.B. Segmentierung des Netzes und Minimierung der Übergänge (bspw. mittels physischer Trennung oder VLAN)

b) Vermeidung von offenen Sicherheitslücken beispielsweise mittels:

- Patchmanagement (Aktualisierungen zur eingesetzten Software müssen stets kurzfristig installiert werden, um entdeckte Schwachstellen zu beheben)
- Härtung von bestehenden Produkten und Plattformen (z.B. Website und Onlineshop, Plug-In-Aktualisierung, Sicherheitszertifikate prüfen)
- Stärkere Abwehrmechanismen in aktuellerer Software, Durchführung von Updates
- Erstellen von Workarounds und Routinen für Sicherheitsaktualisierungen
- Regelmäßige Überprüfung der verwendeten Systeme
- Fehlkonfigurationen prüfen und beheben
- Schwachstellenmanagement

- Analyse der IT-Sicherheitsmaßnahmen des Internetauftritts oder Onlineshops / Etablierung eines Sicherheitslifecycles (kein Neuaufsetzen des Internetauftritts, sondern Verbesserung der bestehenden Struktur)
- Technische Schnittstellenkontrolle auf Client-Systemen, Servern oder anderen IT-Systemen

A3. Vorbereitung auf Sicherheitsvorfälle und Simulation/Planbesprechungen von diesen

a) Beratung hinsichtlich einer individuellen Back-Up Empfehlung (wie würde die Strategie aussehen, wenn der Ernstfall eintritt?)
b) Desaster Recovery
c) Erstellen eines Notfallplans / Handlungsempfehlungen, inkl. Festlegung von Zuständigkeiten für den Fall eines Sicherheitsvorfalls im Bereich der IT-Sicherheit
d) Überprüfung der Vorbereitungsmaßnahmen auf fiktive Angriffe wie bspw. Ransomware-Befall.
e) Planbesprechungen und Übungen dienen dazu, das Vorbereitete zu prüfen und die Sensibilisierung zu verstetigen

Schwerpunkt B: Faktor Mensch - nutzerorientierte Maßnahmen

B1. Sensibilisierung und Schulung der Mitarbeitenden

Der Schwerpunkt adressiert verschiedene Schulungsmaßnahmen, um Mitarbeitende für Themen rund um die Digitale Sicherheit zu sensibilisieren. Ziel ist es, die durch Mitarbeitende verursachten Gefahren zu minimieren und Verhaltens- und Handlungsoptionen aufzuzeigen.
Hierbei sind wiederkehrende Schulungen und Sensibilisierungsmaßnahmen sowie deren Auffrischung innerhalb des Förderzeitraums förderfähig. Eine Schulung kann für Kleingruppen auch auf mehrere Tage verteilt werden.

B2. Festlegung von Zuständigkeiten

Das auftragnehmende Unternehmen kann hier in folgenden Punkten beraten und unterstützen:

a) Definition der technischen und organisatorischen Rollen im Unternehmen
b) Klärung von Verantwortlichkeiten eines jeden Einzelnen
c) Festlegung von Zuständigkeiten

B3. Fortbildung von Mitarbeitenden zur/zum IT-Sicherheitsbeauftragten

Förderung der Absolvierung von Zertifikatslehrgängen mit abschließender Prüfung und Zertifizierung im Bereich der digitalen Sicherheit, um die Schwerpunkte 2.1 und 2.2 innerhalb des Unternehmens zu festigen. Dies kann mittels der folgenden Lehrgänge erfolgen:

- Informationssicherheitsbeauftragte/r und Zusatzqualifikation Cybersecurity (beides Angebote von Industrie- und Handelskammern)
- IT-Security-Beauftragte/r, Cyber Security Specialist, IT-Security-Manager/in und IT-Security-Auditor/in (Angebote des TÜV)
- Information Security Officer (DEKRA)

Im Fall der Inanspruchnahme von B3 ist ein zweites auftragnehmendes Unternehmen zugelassen.

Schwerpunkt C: Software für den IT-Basisschutz

C1. Software

a) Antiviren-Software / Anti-Ransomware

b) DDoS-Schutz-Software

c) Back-Up-Software (keine Förderung von Servern, Datenspeichern, Cloudspeichern, Hardware)

d) Installation, Erwerb von Lizenzen sowie die Wartung sind für max. 12 Monate förderfähig

Software, für die gemäß der Warnungsliste des BSI eine Warnung ausgesprochen wurde, ist von der Förderung ausgeschlossen. Dies gilt auch für bereits archivierte Warnungen.