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

<u>Schwerpunkt B: Faktor Mensch - nutzerorientierte Maßnahmen</u>

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.