Anlage
(zu Nummer 2)

1
Förderfähige Maßnahmen und Lösungen
Hierbei handelt es sich um die abschließende Auflistung von förderfähigen Maßnahmen im Teilprogramm MID-Digitale Sicherheit in den drei Schwerpunkten A, B und C. Die einzelnen Maßnahmen sind beliebig kombinierbar.

1.1
Schwerpunkt A: Analyse des IST-Zustandes der IT-Infrastruktur in der Organisation

Förderfähige Maßnahmen zur Analyse der zu schützenden Infrastruktur als Basis zur Durchführung und Planung weiterer Maßnahmen beziehungsweise Sicherheitsassessments umfassen:
a) Analyse der bereits bestehenden IT-Schutzmaßnahmen,
b) Durchführung einer herstellerneutralen Cyber-Sicherheitsberatung,
c) Penetrationstests durch Simulation von externen Angriffen oder interner Penetrationstest und
d) Aufnahme des IST-Zustands, Interne Schwachstellenüberprüfungen durch IT-Dienstleistung im Sinne der unten aufgeführten Punkte:
aa) Aufnahme des IST-Zustandes, durch Aufnahme der verschiedenen IT-Infrastrukturen,
bb) Überblick und Überprüfung der aktuell verwendeten IT-Systeme,
cc) Überprüfung der Notwendigkeit der vorhandenen IT-Systeme und
dd) IST-Zustand Netzstrukturaufnahme und Identifikation von Netzübergängen, beispielsweise individuelle DSL-Zugänge oder selbst eingerichtete VPN-Zugänge.

Förderfähige Maßnahmen zur Behebung der erkannten Schwachstellen und Sicherheitslücken durch Verbesserung der eingesetzten IT-Systeme umfassen:
a) Dienstleistungen zur Anpassung oder Neustrukturierung der Netzumgebung zur Erhöhung der Schutzwirkung, wie zum Beispiel die Segmentierung des Netzes und Minimierung der Übergänge mittels physischer Trennung oder VLAN,
b) Vermeidung von offenen Sicherheitslücken mittels einmaliger Dienstleistung und Befähigung des antragstellenden Unternehmens zur eigenständigen Durchführung von
aa) Härtung von bestehenden Produkten und Plattformen, wie zum Beispiel Website und Onlineshop, Plug-In-Aktualisierung oder Prüfung von Sicherheitszertifikaten,
bb) stärkere Abwehrmechanismen in aktuellerer Software, Durchführung von Updates und
cc) Erstellen von Workarounds und Routinen für Sicherheitsaktualisierungen oder Patch-Management,
c) Prüfung und Behebung von Fehlkonfigurationen,
d) Schwachstellenmanagement,
e) Analyse der IT-Sicherheitsmaßnahmen des Internetauftritts oder Onlineshops und Etablierung eines Sicherheitslifecycles oder
f) technische Schnittstellenkontrolle auf Client-Systemen, Servern oder anderen IT-Systemen.

Förderfähige Maßnahmen zur Vorbereitung auf Sicherheitsvorfälle und deren Simulation beziehungsweise Planbesprechungen umfassen:
a) Beratung hinsichtlich einer individuellen Back-Up Empfehlung,
b) Desaster Recovery,

c) Erstellen eines Notfallplans und Handlungsempfehlungen, inklusive der Festlegung von Zuständigkeiten für den Fall eines Sicherheitsvorfalls im Bereich der IT-Sicherheit,
d) Überprüfung der Vorbereitungsmaßnahmen auf fiktive Angriffe wie beispielsweise ein Ransomware-Befall oder
e) Planbesprechungen und Übungen, um das Vorbereitete zu prüfen und die Sensibilisierung zu verstetigen.

1.2
Schwerpunkt B: Faktor Mensch - nutzerorientierte Maßnahmen

1.2.1
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. Für die Dienstleistungen zur Sensibilisierung und Schulung werden ausschließlich branchenübliche Tagessätze anerkannt.

1.2.2
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 und
c) Festlegung von Zuständigkeiten.

1.2.3
Fortbildung von Mitarbeitenden zu IT-Sicherheitsbeauftragten
Förderung der Teilnahme von Lehrgängen mit abschließender Prüfung und Zertifizierung als IT-Sicherheitsbeauftragte. Dies muss mittels zertifizierter Fortbildung und Abschluss nach DIN EN ISO/IEC 27001:2023 erfolgen. Im Fall der Inanspruchnahme ist ein zweites auftragnehmendes Unternehmen zugelassen. Die Fortbildung muss dabei zur Steigerung der internen IT-Sicherheit beantragt werden, eine Fortbildung zur späteren Erweiterung der Dienstleistungen ist nicht möglich.

1.3
Schwerpunkt C: Software und Hardware für den IT-Basisschutz
Förderfähige Maßnahmen umfassen die erstmalige Einführung folgender Soft- und Hardware:
a) Antiviren-Software beziehungsweise Anti-Ransomware,
b) schlüsselfertige Firewall, welche als eigenständiges Produkt erworben wird,
c) Software zur eigenständigen Durchführung von Sicherheitsupdates, wie Patch-Management-Software,
d) Backup-Software, ohne Server, Datenspeicher, Cloudspeicher und Hardware,
e) Software zur Durchführung von kontinuierlichen Awareness-Trainings im Bereich der IT-Sicherheit oder
f) Installation und Erwerb von Lizenzen sowie Software-as-a-Service-Lösungen für Antiviren-Software der unter 2.3
Schwerpunkt **C** gelisteten Maßnahmen für maximal 36 Monate, wobei Verlängerungen bereits bestehender Lizenzen hierbei ausgeschlossen sind.

Software für die gemäß der Warnungsliste des Bundesamts für Sicherheit in der Informationstechnik eine Warnung ausgesprochen wurde, ist von der Förderung ausgeschlossen. Dies gilt auch für bereits archivierte Warnungen.
Ausgaben für die Lizenzverträge und Schulungen können nach Absprache mit dem auftragnehmenden Unternehmen in Vorkasse für maximal 36 Monate geleistet werden und entsprechend mit dem Projektabschluss eingereicht werden.
Zulässig ist ausschließlich die erstmalige Beschaffung einer Soft- und Hardware in einem förderfähigen Anwendungsbereich. Dies beinhaltet keine Updates, Erneuerungen von Lizenzen und Hersteller- oder Anbieterwechsel.

2
Nicht förderfähige Maßnahmen und Lösungen
Nicht förderfähige Maßnahmen und Lösungen sind:
a) Koordinierende oder allgemeine Projektmanagement-Tätigkeiten,
b) Einsatz eigener Arbeitskapazitäten,
c) Updates, Erneuerungen von Lizenzen und Wechsel zwischen Hersteller und Anbieter,
d) Zwei-Faktor-Authentifizierung,
e) Standard-IKT-Hardware, wie Server, PCs, Monitore, Laptops, Tablets, Smartphones, Drucker oder Telefone,
f) Komponenten zur Einrichtung von WLAN,
g) Ausgaben für Maßnahmen im Rahmen von Auditierungen,
h) Abschluss von Wartungsverträgen zur Pflege der Systemlandschaft und deren Komponenten oder
i) Reise- und Unterbringungskosten.