Leistungsbeschreibung - Praxis Protect L

1 Präambel 1
2 Technische Voraussetzungen 1
3 Installationsvorraussetzungen 2
4 Installationstermine 2
4.1 Installation UTM – Firewall 3
4.2 Installation managed Workplace 3
5 Leistungsumfang managed Workplace 3
5.1 Fernwartung 4
5.2 Tägliches Monitoring 4
5.3 Systempflege 4
5.4 Patchmanagement und Sicherheitsupdates 4
5.5 Datensicherung 5
5.6 Festplattenverschlüsselung 5
6 Leistungsumfang UTM - Firewall 6
6.1 Leistungsumfang der Hardware Geräte 6
6.1.1 Firewall 6
6.1.2 Access Point 7
6.2 Konfiguration und sicherheitsgerechtes Onboarding 7
6.3 Managed Service Leistungen 7
6.4 Datensicherung der Konfiguration 8
6.5 Installation von Firmware-Updates 8
6.6 Aufbewahrung von Firewall-Protokollen 8
7 Leistungsbeschreibung Endpoint Protection 8
7.1 Zielsetzung und Umfang 8
7.2 Erweiterter Schutz 9
7.3 Vorkonfiguration & Sicherheitseinstellungen 9
8 Service und Support 10
9 Kündigungsfrist 10

1 Präambel

Mit **Praxis Protect L** steht Ihnen eine umfassende Lösung zur Verfügung, die psychotherapeutische Praxen bei der Einhaltung der IT-Sicherheitsrichtlinien der Kassenärztlichen Bundesvereinigung (KBV) wirkungsvoll unterstützt. Angesichts der hohen Anforderungen an den Schutz sensibler Gesundheitsdaten leistet **Praxis Protect L** einen wichtigen Beitrag zur **sicheren und gesetzeskonformen** Praxisführung.

Das Produkt setzt sich aus drei wesentlichen Leistungsbestandteilen zusammen: dem **managed Workplace, einer UTM-Firewall und einer Endpoint Protection**. Diese Bausteine ergänzen sich zu einem ganzheitlichen Sicherheitskonzept, das auf die typischen IT - Anforderungen in psychotherapeutischen Praxen abgestimmt ist.

Im Folgenden werden die Leistungsbestandteile und die hierfür notwendigen technischen Voraussetzungen genauer beschrieben.

2 Technische Voraussetzungen

Damit wir Ihre Geräte zuverlässig betreuen können, müssen diese folgende Mindestanforderungen erfüllen:

- Windows 10 Professional oder neuer
- Prozessor mit mindestens 4 Kernen und 1,8 GHz
- 8 GB Arbeitsspeicher
- 240 GB SSD-Festplatte
- Eine stabile **Breitband – Internetverbindung von mindestens 5 Mbit.**
- Administratorrechte zur Installation unserer Software
- Ihre Kontaktdaten

Falls Ihre vorhandene Hardware nicht geeignet ist, bieten wir passende Praxis PC‘s zur Miete oder zum Kauf an.

3 Installationsvorraussetzungen

Die gelieferte Hardware (Firewall sowie Access Point) muss vollständig und in der Praxis vorhanden sein.
Zur **Firewall** müssen folgende Komponenten im Originalumfang enthalten sein:

- Cloud-PIN
- Netzanschluss
- LAN-Kabel

Diese Bestandteile sind originalverpackt im Lieferumfang enthalten. **Sie dürfen bis zum Onboarding-Termin nicht entnommen werden**, sondern müssen vollständig und unversehrt in der Verpackung verbleiben. **Sollten Bestandteile fehlen oder durch vorheriges Öffnen der Verpackung unauffindbar sein und dadurch das Onboarding nicht ordnungsgemäß durchgeführt werden können, trägt der Auftraggeber die daraus entstehenden Kosten für den Techniker-Einsatz.**

Beim **Access Point** müssen folgende Komponenten in der Verpackung vorhanden sein:

- Cloud-PIN
- Netzanschluss
- LAN-Kabel
- Montagezubehör

Diese Bestandteile sind originalverpackt im Lieferumfang enthalten. **Sie dürfen bis zum Onboarding-Termin nicht entnommen werden**, sondern müssen vollständig und unversehrt in der Verpackung verbleiben.

Sollten Bestandteile fehlen oder durch vorheriges Öffnen der Verpackung unauffindbar sein und dadurch das Onboarding nicht ordnungsgemäß durchgeführt werden können**, trägt der Auftraggeber die daraus entstehenden Kosten für den Techniker-Einsatz.**

4 Installationstermine

Die einmaligen Kosten für die Installation des Pakets Praxis Protect L belaufen sich derzeit auf **899 € netto**. Die Installation teilt sich in **zwei verschiedene Installationstermine** auf.

4.1 Installation UTM – Firewall

- Zur Installation der UTM – Firewall wird mit Ihnen ein Installationstermin vereinbart. Die Einsatzdauer der Installation beträgt zwei Stunden. Für die erfolgreiche Installation müssen, die in **Punkt 3** beschriebenen Installationsvorraussetzungen erfüllt sein.

In dem angegebenen Installationszeitraum werden folgende Leistungsbestandteile erfüllt.

- Anschluss der UTM – Firewall an Ihr bestehendes Netzwerk
- Anschluss des Access Points an Ihr bestehendes Netzwerk
- Anschluss eines Switches an Ihr bestehendes Netzwerk
- Konfigurierung der installierten Geräte
- Installation der notwendigen UTM – Firewall Sicherheitszertifikate auf Ihrem Endgerät

Sollte durch den Kunden ein zusätzlicher Aufwand im Zusammenhang mit einem Installationstermin verursacht werden – etwa durch **nicht vorbereitete Infrastruktur**, **Terminverschiebungen** oder zusätzlichen **technischen Abstimmungsbedarf** – behält sich die HASOMED GmbH vor, den dadurch entstehenden Mehraufwand gesondert in Rechnung zu stellen. Die Kosten belaufen sich hierbei auf **16 Euro netto je angefangene 15 Minuten**.

4.2 Installation managed Workplace

Zur Installation des **managed Workplace** wird mit Ihnen ein separater **Installationstermin per Fernwartung** durchgeführt. Für diesen Termin müssen Sie einen PC bereitstellen, der den beschriebenen technischen Voraussetzungen aus **Punkt 1** entspricht.

5 Leistungsumfang managed Workplace

Mit **managed Workplace** wird Ihnen ein sogenannter ***Managed Service*** für Ihren PC geboten, der zentrale Sicherheitsfunktionen kontinuierlich überwacht, aktualisiert und verwaltet – ohne zusätzlichen Aufwand für Sie. So wird sichergestellt, dass Ihre Systeme stets den aktuellen Sicherheitsstandards entsprechen und zuverlässig vor Bedrohungen geschützt sind. Unser Ziel ist es Sie bei der Umsetzung der **IT-Sicherheitsrichtlinien der KBV** bestmöglich zu unterstützen. Im Folgenden erhalten Sie eine detaillierte Beschreibung der enthaltenen Leistungsbestandteile

5.1 Fernwartung

- Wir können Ihre Geräte bei Problemen aus der Ferne warten – schnell, sicher und datenschutzkonform.
- Dafür installieren wir ein spezielles Fernwartungstool auf Ihren Geräten.
- Alle unsere Techniker sind zur Verschwiegenheit verpflichtet.

5.2 Tägliches Monitoring

Ihre Geräte werden täglich automatisch überprüft. Dabei wird geprüft:

- Die Lauffähigkeit der Windows - Dienste
- Mögliche Überschreitungen des Festplattenfüllstandschwellwertes
- Aktualität der Anti – Virus Signaturen,
- Ob kritische Fehlermeldungen vorliegen
- Ob die Festplatte technisch in Ordnung ist

5.3 Systempflege

Einmal im Monat werden automatisch:

- Temporäre Dateien gelöscht
- Der Internet-Browser-Cache geleert
- Alte Systemmeldungen (Eventlogs) entfernt

5.4 Patchmanagement und Sicherheitsupdates

- Bereitstellung & Betrieb einer Software zur Schwachstellenanalyse sowie Installation von Microsoft- und Drittanbieter-Sicherheitsupdates
- Tägliche Installationsroutinen auf den Arbeitsplätzen, inkl. erforderlicher Neustarts.
- Wartungsfenster werden vom Kunden zur Verfügung gestellt.
- Erfolgsprüfung der Updates erfolgt täglich. Die Ergebnisse sind im IT-Management-System des Auftragnehmers einsehbar.
- Haftungsausschluss: Für Fehlerfreiheit, Risiko-Klassifizierung und Kompatibilität der Updates ist ausschließlich der jeweilige Softwarehersteller verantwortlich.

- Hinweis an Endkunden: Updates können Funktionsveränderungen verursachen, daraus resultierende Probleme liegen nicht in der Haftung des Auftragnehmers. Problemlösungen erfolgen nach gängigen Standards.
- Testverfahren: Sicherheitsupdates werden vorab auf einem vom Kunden benannten Gerät geprüft. Erfolgt innerhalb einer Woche keine Rückmeldung über erhebliche Störungen, gilt die Freigabe für alle Systeme als erteilt.

- Wir kümmern uns täglich um die Installation wichtiger Sicherheitsupdates für Windows und weitere Standardprogramme.

Zum Leistungsumfang dieser Programme gehören zum Beispiel:

- Texteditoren
- Packprogramme
- Office Anwendungen
- PDF-Reader

Die Auswahl der eingesetzten Programme erfolgt nicht statisch, sondern unterliegt einem dynamischen Anpassungsprozess, der sich an technischen Entwicklungen orientiert.

Wir übernehmen keine Haftung für Fehler in den Updates, helfen aber bei Problemen schnell weiter.

5.5 Datensicherung

- Ihre Daten werden täglich gesichert.
- Die Übertragung und Speicherung erfolgt verschlüsselt.
- Die Daten liegen in einem **deutschen Rechenzentrum** mit höchsten Sicherheitsstandards, die gemäß SOC-2, ISO 27001 und PCI-DSS zertifiziert sind.

5.6 Festplattenverschlüsselung

- Die Festplatten Ihrer Geräte werden vollständig verschlüsselt – mit Microsoft BitLocker.
- So sind Ihre Daten auch bei Diebstahl oder Verlust vor unbefugtem Zugriff geschützt.
- Die Verantwortung für die sichere Aufbewahrung und Verwaltung des **Wiederherstellungscodes** sowie des **PINs zur Entschlüsselung der Daten** obliegt ausschließlich der Praxis. Die HASOMED GmbH übernimmt keine Haftung für deren Verlust oder die daraus resultierenden Folgen.

6 Leistungsumfang UTM - Firewall

Diese Leistung beinhaltet eine **Firewall** und einen **Access Point**. Zusätzlich kümmert sich unser Expertenteam um die installationsgerechte Konfiguration, sowie betriebsgerechte Wartung der genannten Hardware. Es bietet Ihnen einen effektiven Schutz für Ihre Netzwerkstruktur und gewährleistet eine zuverlässige und sichere Internetverbindung für Ihre Praxis.

6.1 Leistungsumfang der Hardware Geräte

Der folgende Abschnitt beschreibt die Leistungsumfänge der eingesetzten Hardware im Detail. Hierzu zählen die **Firewall** zur Absicherung des Netzwerks sowie der **Access Point** für eine leistungsstarke und zuverlässige WLAN-Versorgung.

6.1.1 Firewall

Die **Firewall** schützt Ihr Netzwerk vor unerwünschten Zugriffen und bietet einen umfassenden Schutz vor externen Bedrohungen.

Zu den Funktionen gehören:

- **Datenbankbasierter Schutz vor bekannten Bedrohungen**: Erkennung und Blockierung bekannter Malware und Cyberangriffe durch eine ständig aktualisierte Bedrohungsdatenbank.
- **Schutz vor unbekannten Bedrohungen mit Sandboxing und Machine Learning**: Verdächtige Dateien werden in einer isolierten Umgebung (Sandbox) analysiert, bevor sie ins Netzwerk gelangen. Künstliche Intelligenz hilft dabei, neue Bedrohungen zu identifizieren und zu stoppen.
- **DPI-basierte Kontrolle über Anwendungen und Inhalte**: Deep Packet Inspection (DPI) ermöglicht eine detaillierte Analyse des Datenverkehrs, um Anwendungen und Inhalte gezielt zu kontrollieren oder zu blockieren.
- **Filterung des Netzwerkverkehrs**: Identifikation und Blockierung unerwünschter oder schädlicher Netzwerkaktivitäten.
- **Inhaltsbasierte Filter zum Schutz vor Phishing-Angriffen**: Schutzmechanismen zur Erkennung und Blockierung von Phishing-Versuchen und gefährlichen Webseiten.

6.1.2 Access Point

Der **Access Point** sorgt für eine stabile und sichere WLAN-Verbindung in Ihrem Unternehmen. Zu den Hauptmerkmalen gehören:

- **WLAN-Management**: Automatische Konfiguration und Optimierung der WLAN-Verbindung.
- **Verschlüsselung**: WPA3-Verschlüsselung für sicheren Drahtloszugriff.
- **WLAN-Sicherheit**: Schutz vor unbefugtem Zugriff auf Ihr WLAN-Netzwerk.
- **Roaming**: Nahtloses WLAN ohne Verbindungsabbrüche innerhalb des Netzwerks.
- **Sicherheit für drahtlose Netzwerke**: Höchste Sicherheitsstandards für WLAN, um unbefugten Zugriff zu verhindern und die Datenübertragung abzusichern.

6.2 Konfiguration und sicherheitsgerechtes Onboarding

Unsere Experten richten die Firewall und den Access Point nach Ihren Praxis - Anforderungen ein. Folgende Punkte werden bearbeitet

- Erstellung und Dokumentation eines Netzplans
- Konfiguration der Hardware-Geräte, angepasst auf Ihre Praxis IT
- Einspielen von Firewall – Regeln zum Schutz Ihres Netzwerks
- Installation von Sicherheitszertifikaten auf Ihrem System PC

6.3 Managed Service Leistungen

Um die Sicherheit und Verfügbarkeit Ihrer IT-Infrastruktur kontinuierlich zu gewährleisten, bieten wir in Kooperation mit unserem IT – Dienstleister LOOMA GmbH einen managed Service über eine Cloud an. Dieser Service umfasst folgende Funktionen:

- Monitoring der Firewall sowie Einspielen globaler Regeln und Firmware-Updates
- Zentrale Überwachung der Verfügbarkeit und Telemetriedaten
- Einspielen von **getesteten Updates** zur Optimierung der Sicherheit
- Laufende Updates basierend auf **Datenbanken des BSI** und weiteren Sicherheitsquellen
- Automatische Alarmierung des IT – Dienstleisters bei entdeckten Sicherheitsproblemen

6.4 Datensicherung der Konfiguration

- Monatliche Sicherung der Firewall-Konfiguration
- Speicherung der **letzten drei Sicherungen** in einem deutschen Rechenzentrum

6.5 Installation von Firmware-Updates

- **Tägliche, automatisierte Sicherheitsupdates**
- **Monatliche Firmware-Updates** mit geplantem Neustart der Hardware
- Updates erfolgen **außerhalb der Arbeitszeiten (Mo–Fr 08:00–17:00 Uhr)**
- **Keine Haftung für mögliche Inkompatibilitäten** durch Updates
- Problemlösung nach üblichen IT-Standards

6.6 Aufbewahrung von Firewall-Protokollen

- Log-Dateien werden für 90 Tage gespeichert
- Enthaltene Daten:
    - Website-Zugriffe & blockierte Verbindungen
    - Datentransfers & Volumen
    - Alarmmeldungen der Firewall

7 Leistungsbeschreibung Endpoint Protection

Im Folgenden wird der Leistungsumfang des Managed Endpoint Security beschrieben. Dieser umfasst den Schutz vor Schadsoftware rund um Ihren Praxis-PC.

7.1 Zielsetzung und Umfang

Die Lösung stellt sicher, dass Ihr Praxis - PC bestmöglich geschützt ist. Das beinhaltet:

- Schutz vor Viren, Malware und Cyberangriffen
- Regelmäßige Updates
- Einfache Integration in Ihre bestehende IT-Infrastruktur
  Bitte beachten Sie, dass Hardware nicht Bestandteil dieser Leistung ist.

7.2 Erweiterter Schutz

Unsere Managed Endpoint Security schützt ausschließlich die Computer und Server, auf denen sie installiert ist. Sie umfasst:

Unsere Lösung kombiniert zwei leistungsstarke Technologien:

- **Endpoint Protection Platform (EPP):**
  - Automatische Virenscans und Schutz in Echtzeit
  - Individuelle Anpassung von Blacklists & Whitelists
  - Manipulationsschutz und E-Mail-Filterung
- **Endpoint Detection and Response (EDR):**
  - Permanente Überwachung aller Aktivitäten
  - Blockierung unbekannter Programme, bis diese als sicher eingestuft wurden
  - Automatische Bedrohungsanalyse durch künstliche Intelligenz

7.3 Vorkonfiguration & Sicherheitseinstellungen

- **Sandboxing:** Unbekannte Dateien werden in einer gesicherten Umgebung getestet.
- **Anti-Exploit-Technologie:** Schutz vor Hackerangriffen durch Schwachstellen.
- **Virenschutz:** Automatische Erkennung und Blockierung von Bedrohungen.
- **Content-Filter:** Steuerung des Internetzugriffs Ihrer Mitarbeiter.
- **Threat Hunting Service:** Proaktive Analyse verdächtiger Aktivitäten.

8 Service und Support

Unser Support-Team steht Ihnen zur Servicezeit gemäß unserer Website Allgemeine Geschäftsbedingungen (AGB) | HASOMED GmbH zur Verfügung. Sie können uns telefonisch oder per E-Mail erreichen, um Service- oder Supportanfragen zu stellen.

9 Kündigungsfrist

Der Vertrag wird für 12 Monate geschlossen (Mindestlaufzeit). Nach Ablauf der Mindestvertragslaufzeit verlängert sich der Vertrag jeweils um zwölf Monate und kann mit einer Frist von drei Monaten zum Ende der jeweiligen Vertragslaufzeit gekündigt werden. Das Recht zur außerordentlichen Kündigung bleibt davon unberührt