Leistungsbeschreibung – Praxis Protect M

1 Präambel

Sehr geehrte Damen und Herren,

vielen Dank, dass Sie sich für unser Produkt **Praxis Protect M** entschieden haben. Dieses umfassende Sicherheitspaket beinhaltet eine **UTM-Firewall** und einen **Access Point**. Unser Expertenteam übernimmt sowohl die fachgerechte Installation als auch die betriebsbereite Wartung der Hardware. So erhalten Sie einen effektiven Schutz für Ihre Netzwerkstruktur und eine zuverlässige, sichere Internetverbindung für Ihre Praxis.

Zusätzlich umfasst dieses Angebot die Installation einer **Endpoint Protection** (Virenschutz) auf Ihrem Praxis-PC.

Im Folgenden finden Sie eine detaillierte Beschreibung der enthaltenen Leistungen und Rahmenbedingungen.

2 Technische Voraussetzungen

Für die optimale Nutzung von Praxis Protect M benötigen Sie:

- Eine stabile Breitband-Internetverbindung von **mindestens 5Mbit**.

Folgende Betriebssysteme werden unterstützt:

- **Windows:** ab Windows 10
- **MacOS:** ab Version 10.10

3 Installationsvorraussetzungen

Damit **Praxis Protect M** betriebsgerecht installiert werden kann, müssen folgende Bedingungen erfüllt sein:

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 Kunde 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 Kunde die daraus entstehenden Kosten für den Techniker-Einsatz.**

4 Installationstermine

Die einmaligen Kosten für einen Technikereinsatz belaufen sich derzeit auf **699 € netto**. Dieser Betrag umfasst eine Einsatzdauer von **bis zu 2 Stunden**.

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 Endpoint Protection

Zur Installation der **Endpoint Protection** wird mit Ihnen ein **Installationstermin per Fernwartung** durchgeführt. Für diesen Termin müssen Sie einen PC bereitstellen, der den beschriebenen technischen Voraussetzungen aus **Punkt 2** entspricht.

5 Leistungsumfang der Hardware-Geräte

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

5.1 UTM - 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.

5.2 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 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

7 Managed Service Leistungen

Um die Sicherheit und Verfügbarkeit Ihrer IT-Infrastruktur kontinuierlich zu gewährleisten, bieten wir 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

8 Datensicherung der Konfiguration

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

Kommentiert [TK1]: in einem deutschen Rechenzentrum

9 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

10 Aufbewahrung von Firewall-Protokollen

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

11 Leistungsbeschreibung Endpoint Protection (Virenschutz)

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

11.1 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.

11.2 Erweiterter Schutz

Unsere **Endpoint Protection** 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

11.3 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.

12 wichtiger Hinweis

Die **Firewall**, der **Access Point** sowie die **Endpoint Protection** bieten einen umfassenden Schutz für Ihr Netzwerk und Ihren Praxis-PC, jedoch kann keine **100%ige Sicherheitsgarantie** gewährleistet werden. Die KBV IT – Sicherheitsrichtlinie wird durch die Implementierung der Firewall teilweise erfüllt, zur vollständigen Erfüllung der weiteren Anforderungen sind zusätzliche Maßnahmen notwendig. Sie können die KBV – IT-Sicherheitsrichtlinien unter folgendem Link vorfinden:

Praxishinweise - Richtlinie IT-Sicherheit in der Praxis - IT in der Versorgung

13 Service und Support

Kommentiert [MS2]: Wie wollen wir hier das SLA definieren?

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.

14 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