Leistungsbeschreibung CGM TELEMED Protect Platin

Gegenstand dieser Leistungsbeschreibung

Die CompuGroup Medical Deutschland AG, Geschäftsbereich TELEMED (im Folgenden TELEMED genannt), bietet mit den TELEMED Protect Paketen IT-Security-Bundles an, deren Zusammensetzung und Leistungen nachfolgend beschrieben sind. Dabei können unter Ziffer 1 Allgemeine Informationen entnommen werden. Unter Ziffer 2 werden diejenigen Leistungsbestandteile beschrieben, welche zum Schutze des Endpoints (PC-Arbeitsplatz oder Server) in das Paket integriert wurden. Mittels der unter Ziffer 3 dargestellten Online Produkte wird der Online-Zugang vor Ausfällen und Bedrohungen aus dem Internet geschützt. Das Platin-Paket enthält zudem das unter Ziffer 4 beschriebene Investitionsversprechen, welches den Auftraggeber im dort genannten Umfang vor erneuten Investitionen für die Umsetzung der IT-Sicherheitsrichtlinie gemäß §75b Abs. 1, SGB V schützen soll. Ziffer 5 beschreibt den Umgang mit nachträglichen Anpassungen auf Wunsch des Auftraggebers und unter 6 wird der Service Level definiert.

1. Allgemeine Informationen

1.1 Hardware

Sofern für die Leistungserbringung gemäß dieser Leistungsbeschreibung spezielle Hardware benötigt wird, stellt TELEMED diese dem Auftraggeber zur Verfügung. Davon ausgeschlossen ist der Konnektor der Telematikinfrastruktur, welcher für TELEMED Connect SIS benötigt wird sowie spezielle Modems für Kabel- und Glasfaserinternetanschlüsse, die vom Auftraggeber gestellt werden. Insbesondere Arbeitsplatzcomputer, Netzwerke und / oder Laptops verstehen sich nicht als spezielle Hardware gemäß dieser Leistungsbeschreibung, die von TELEMED bereitzustellen ist.

Datenblätter mit genauen Spezifikationen der von TELEMED gemäß dieser Leistungsbeschreibung zur Verfügung gestellten Hardware können jederzeit unter www.cgm.com/telemed-download eingesehen werden.

1.2 Anzahl der PC-Arbeitsplätze

Grundsätzlich können beliebig viele PC-Arbeitsplätze mit den TELEMED Protect Paketen geschützt werden. Das jeweils einzelne Paket umfasst den Schutz von bis zu fünf PC-Arbeitsplätzen.

1.3 Systemvoraussetzungen für die Endpoint-Produkte

Die Security-Software der TELEMED Protect Pakete wird direkt auf den Client-PC und Servern des Auftraggebers implementiert. Es gelten die folgenden Systemvoraussetzungen:

Windows-Workstations:
Windows 8.1, Windows 10

Windows-Server:
2012 R2, 2016, 2019

MacOS-Workstations und -Server:
MacOS (ab Version 10.10)

1.4 Voraussetzungen für die Online-Produkte

Vom Auftraggeber zu stellende Voraussetzung für Installation und Nutzung der Online-Produkte (siehe Punkt 3.) dieser Leistungsbeschreibung ist ein breitbandiger Internetanschluss: ADSL (2/2+) oder VDSL (-Vectoring). Die Nutzung von alternativen Breitband-Internetanschlüssen ist ebenfalls möglich, jedoch müssen diese mittels geeignetem, vom Auftraggeber bereitgestellten Modem per Ethernet-Schnittstelle an TELEMED übergeben werden.

2.0 Enthaltene Endpoint-Produkte

Leistungsbestandteile, welche lt. dieser Leistungsbeschreibung den Endpoint-Produkten zuzuordnen sind, schützen mit den beschriebenen Leistungen ausschließlich den Computer (Arbeitsplatz oder Server) auf dem sie installiert sind.

2.1 TELEMED Protect Endpoint Pro

TELEMED Protect Endpoint Pro ist eine Kombination aus einer Endpoint-Protection-Platform (EPP), die eine traditionelle Antivirensoftware enthält, und zusätzlich einen State-of-the-Art-Endpoint-Schutz mit einem cloudbasierten Endpoint-Detection-and-Response-Dienst (EDR) kombiniert. TELEMED Protect Pro klassifiziert alle Portable Executables im Zusammenhang mit Parent- und Child-Prozessen und stuft diese als vertrauenswürdig, schädlich oder unbekannt ein. In Verbindung mit TELEMED Protect Sandbox wird jede Art von Schadsoftware registriert, da nach der Klassifizierung alle als unbekannt eingestuften Portable Executables im Zusammenhang mit Parent- und Child-Prozessen in gesicherter Umgebung analysiert werden (siehe auch 2.2). Wenn die Schadsoftware bereits auf dem System des Auftraggebers vorhanden war, bevor TELEMED Protect Endpoint Pro installiert wurde, ermöglicht die Echtzeitüberwachung die Erkennung, sobald die Schadsoftware aktiv wird und liefert Informationen darüber, was sie seit der Installation von TELEMED Protect Endpoint Pro getan hat. TELEMED Protect Endpoint Pro bedient sich dabei der folgenden Methoden:

2.1.1 Traditionelle Präventionsmethoden

- Gerätesteuerung
- Ständige Multi-Vektor-Scans zur Malware-Erkennung, auch on- Demand
- Managed Blacklisting / Whitelisting
- Vor-Ausführungs-Heuristik
- Internetzugriffskontrolle
- Spam- und Phishingschutz
- Manipulationsabwehr
- Mail-Inhaltsfilter

2.1.2 State of the Art Sicherheitstechnologien

- EDR: ständige Überwachung der Endpointaktivität
- Verhindert die Ausführung unbekannter Prozesse, bis diese als vertrauenswürdig eingestuft werden, oder eine manuelle Freigabe auf Wunsch des Auftraggebers durch TELEMED erfolgt
- Cloudbasiertes maschinelles Erlernen von Verhaltensweisen ermöglicht die Klassifizierung sämtlicher unbekannter Prozesse (APT, Erpressungssoftware, Rootkits, etc.)
- Cloudbasiertes Sand Boxing in realen Umgebungen
- Verhaltensanalysen und Indicator-of-Attack-Erkennung (Skripte, Makros etc.)
- Automatische Erkennung und Abwehr von Arbeitsspeicher- Exploits
- Managed Threat Hunting bei Angriffen ohne Malware

2.2 TELEMED Protect Sandbox

TELEMED Protect Sandbox ist Bestandteil von TELEMED Protect Endpoint Pro und verfügt über verschiedene Modi. TELEMED setzt dabei, im Rahmen der Protect Pakete, ausschließlich auf den unten beschriebenen Hardening-Modus. Dabei werden potentielle Bedrohungen durch Sandboxing in einer kontrollierten Umgebung überwacht. Da der Schadcode diese Umgebung i. d. R. nicht von einem regulären Server- oder

Arbeitsplatzbetriebssystem unterscheiden kann, versucht er in der kontrollierten Umgebung das zu tun, wofür er programmiert wurde, wie z. B. Daten zu beschädigen oder verschlüsseln. Dies ermöglicht es unbekannte Dateien nach ihren Verhaltensmustern zu klassifizieren und entsprechend der hinterlegten Logik für den Umgang mit bekannten Dateien zu blockieren oder zuzulassen. TELEMED Protect Endpoint Pro überwacht den Endpoint permanent, erkennt automatisch Bedrohungen und blockiert diese. Alle Daten zum Applikationsverhalten werden lokal nur zwischengespeichert, die Auswertung erfolgt in einer Cloud-Umgebung.

Hardening Modus:
Schädliche Programme werden entfernt. Unbekannte und somit potentiell schädliche Programme, die aus dem Internet, von anderen Netzwerkcomputern oder von externen Laufwerken stammen, werden blockiert, bis mittels des cloudbasierten Sandboxings bestimmt wurde, ob es sich um Schadsoftware handelt oder nicht. Andere unbekannte Programme, z. B. solche die sich bereits vor der Installation von TELEMED Protect Sandbox auf dem PC befunden haben, werden zunächst zur Ausführung zugelassen, während sie in der cloudbasierten Sandbox analysiert werden.

2.3 TELEMED Protect Monitoring

Der TELEMED Protect Monitoring Dienst wird auf den PC-Arbeitsplätzen installiert und übermittelt fortlaufend die nachbenannten Informationen an TELEMED damit potentielle Systemausfälle frühzeitig erkannt werden oder im Fall eines Ausfalls schnell reagiert werden kann. Zu diesem Zweck sendet TELEMED Protect Monitoring den Status zur Erreichbarkeit des Servers und der Arbeitsplatz-Computer sowie deren Festplattenkapazität an die zentralen TELEMED-Monitoring-Server. Zudem wird im Intervall von 5 Minuten geprüft ob der Dienst TELEMED Protect Endpoint Pro inkl. TELEMED Protect Sandbox aktiv ist.
Sobald die Festplatte die unter 2.3.1 definierte Auslastung erreicht, der PC ausfällt (siehe 2.3.3) oder TELEMED Protect Endpoint Pro deaktiviert wird (2.3.2), erfolgt automatisch eine Benachrichtigung per E-Mail an die vom Auftraggeber im Bestellschein angegebene E-Mail-Adresse.
Es gelten die unter 2.3.1 - 2.3.3 definierten Prüfintervalle und Grenzwerte:

2.3.1 Festplattenkapazität:

Intervall: 15 Minuten
Prüfobjekt: Festplatten
Prüfattribut: "Disk Free (GB)"
Benachrichtigung:
Warnmeldung bei >= 10GB und < 20GB freier Platz
Kritische Meldung bei < 10GB freier Platz

2.3.2 TELEMED Protect Endpoint Pro:

Intervall: 5 Minuten
Prüfobjekt: Panda Services (Cloud Antivirus, Endpoint Agent, Product Service)
Prüfattribut: Status des Service
Benachrichtigung:
Kritische Meldung wenn der Service nicht läuft

2.3.3 Erreichbarkeit von Server- und Arbeitsplatzsystemen:

Intervall: 5 Minuten
Prüfobjekt: laufender Prozess der Agent Software
Prüfattribut: meldet sich der Agent in vorgegebener Zeit am Server
Benachrichtigung:
Warnmeldung: 300s-600s
Kritische Meldung: >600s
Benachrichtigungen werden nur für Serverbetriebssysteme verschickt, nicht für Workstations, da Workstations i. d. R. zum Feierabend abgeschaltet werden.

2.4 TELEMED Protect Contentfilter

Der TELEMED Protect Contentfilter ist Bestandteil der TELEMED Protect Endpoint Pro und ist eine Lösung für Web-Sicherheit und Zugriffskontrolle, mit dem die Internetnutzung durch Mitarbeiter reguliert werden kann.
Der TELEMED Protect Contentfilter kann den Aufruf von Websites gezielt steuern und dabei den Zugriff auf bestimmte Inhaltskategorien sperren.
TELEMED gibt hierbei Kategorien vor, welche häufiger mit Sicherheitsrisiken für die Praxis-IT in Verbindung gebracht werden.

Folgende Kategorien werden seitens TELEMED gesperrt:

- Anonymizer
- Bilder von Kindesmissbrauch
- Hacker
- Illegale Software
- Kriminelle Aktivität
- Spamseiten

Die Freischaltung der zuvor genannten Kategorien kann auf schriftlichen Auftrag des Auftraggebers an TELEMED hin erfolgen, sofern die Freischaltung im Einklang mit der IT-Sicherheitsrichtlinie gemäß §75b SBG V steht.

Ebenfalls können bei Beauftragung des Auftraggebers die nachfolgenden Funktionen aktiviert, konfiguriert bzw. freigeschaltet werden, sofern die Freischaltung im Einklang mit der IT-Sicherheitsrichtlinie gemäß §75b SBG V steht:

- Zugriff auf Seiten verweigern, die als unbekannt eingestuft wurden
- Zugriffe auf bekannte/unbekannte Adressen und Domänen können zugelassen (Whitelist-Verfahren) oder verweigert (Blacklist-Verfahren) werden

2.5 TELEMED Protect Patch

TELEMED Protect Patch ist eine Patchmanagement Lösung, welche eine zentralisierte Echtzeit-Sicherheitsstatusübersicht für alle Software-Schwachstellen, fehlende Patches, Updates und nicht mehr unterstützte (EOL) Software bietet, sowie benutzerfreundliche Tools für den gesamten Patch-Management-Zyklus: von der Ermittlung und Planung bis hin zur Installation und Überwachung der Endpoints. TELEMED updatet automatisch mit TELEMED Protect Patch ausschließlich sicherheitsrelevante Updates (Microsoft und Drittanbieter). Eine aktuelle, vollständige Übersicht der Software, welche von TELEMED Protect Patch mit Sicherheitsupdates versorgt wird, wird vom Hersteller unter https://info.pandasecurity.com/patchmanagementapp/ bereitgestellt**.**

Dabei werden alle sicherheitsrelevanten Patches zyklisch installiert. Ein Zyklus entspricht 7 Kalendertagen.

Der Auftraggeber erhält monatlich eine Übersicht der im vergangenen Monat von TELEMED Protect Patch installierten Patches.

2.6 TELEMED Protect DLD

TELEMED Protect DLD ist eine Lösung zur Erkennung von Datenbewegungen auf den Arbeitsplätzen des Auftraggebers, welche mittels verschiedener Software-Module realisiert wird. Ziel ist es den unerwünschten Abgang von personenbezogenen Daten zu erkennen, damit der Auftraggeber im Falle von Datenschutzverstößen angemessen reagieren kann.
Dazu werden in Echtzeit ruhende, verwendete und übertragene unstrukturierte Daten ermittelt, geprüft und überwacht. Bei den unstrukturierten Daten handelt es sich um die nachfolgend klassifizierten, personenbezogenen Daten:

- Vor- und Nachnamen
- Adressen
- E-Mail-Adressen
- Telefonnummern
- Bankkontonummern

Die genannten Daten werden in den folgenden Dateitypen identifiziert, was die anschließende Überwachung ermöglicht:

Dateitypen Microsoft Produkte:

- Windows
  - txt
  - rtf
- Word
  - doc
  - dot
  - docx
  - docm
- Excel
  - xls
  - xlsm
  - xlsx
  - xlsb
  - csv
- Powerpoint
  - ppt
  - pps
  - ppsx
  - ppsm
  - sldx
  - sldm
  - potx
  - pptm
  - pptx
  - potm
- Outlook
  - eml

Dateitypen Browser:

- htm
- html
- mht
- oth

Dateitypen anderer Anbieter:

- pdf
- xml
- Open Office (alle Formate)

Strukturierte Daten:
Da es sich bei Datenbanken um strukturierte, i. d. R. verschlüsselte Daten handelt, welche nicht mittels der, von TELEMED eingesetzten Tools, eingesehen werden können, werden diese als Ganzes auf ihre Bewegung hin überwacht. Es werden Datenbanken mit den folgenden Endungen überwacht:

- .dat
- .idx
- .rcy
- .pdt
- .mdf
- .ndf
- .sql
- .sdf
- .db
- .dbs
- .tmd

Benachrichtigungen:
Im Falle der Übertragung / Löschung / des Kopierens von unstrukturierten, personenbezogenen Daten, oder ganzen Datenbanken erhält der Auftraggeber unmittelbar nach dem Vorgang eine Benachrichtigung an die, bei Bestellung hinterlegte E-Mail-Adresse, mittels welcher er über deren Bewegung informiert wird. Zudem wird dem Auftraggeber wöchentlich eine Übersicht über die Dateien und Computer welche personenbezogenen Daten beinhalten zur Verfügung gestellt.

3.0 Online-Produkte

Leistungsbestandteile welche gemäß dieser Leistungsbeschreibung den Online-Produkten zuzuordnen sind, schützen mit den beschriebenen Leistungen den Online-Zugang und die dahinter befindlichen Komponenten des Praxisnetzwerks.

3.1 TELEMED Protect Firewall Pro

Bei der TELEMED Protect Firewall Pro handelt es sich um Firewall-Lösung zum Schutz des gesamten Praxisnetzwerks vor Bedrohungen von Außerhalb und wird daher dem lokalen Netzwerk physisch vorgeschaltet. Zur Erbringung der nachfolgend definierten Leistungen der TELEMED Protect Firewall Pro setzt TELEMED eine der folgenden technischen Firewall-Lösungen ein:

Hardware-Firewall:
Es wird ein dediziertes Gerät zwischen Einwahlrouter und Praxisnetzwerk gesetzt und sämtlicher Datenverkehr (ein- und ausgehend) durch dieses geleitet. Mittels spezieller Software auf dem zwischengeschalteten Gerät werden die nachfolgend beschriebenen Funktionen und Regeln umgesetzt.

Cloud-Firewall:
Bei einer Cloud-Firewall wird die Firewall-Software auf einem Server außerhalb Praxisnetzwerk ausgeführt. Im Falle der TELEMED Protect Firewall Pro wird der Datenverkehr des Auftraggebers mittels sicherem VPN-Tunnel auf den zuständigen Server geleitet, wo die nachfolgend beschriebenen Funktionen und Regeln umgesetzt werden. Der Aufbau des VPN-Tunnels erfolgt direkt im Einwahlrouter, oder einem zwischen Einwahlrouter und Praxisnetzwerk geschalteten VPN-Gateway.

Unabhängig von der technischen Umsetzung handelt sich dabei immer um eine Next Generation Firewall, welche über nachfolgend von TELEMED definierte Regeln den Datenverkehr in und aus der Praxis reguliert.
Dabei werden sämtliche eingehenden Verbindungen gesperrt und nur diejenigen Ports, welche wirklich benötigt werden, eingehend geöffnet. Ausgehende Verbindungen unterliegen keiner Einschränkung. Der erlaubte, unverschlüsselte Datenverkehr wird, bevor er ins Praxisnetzwerk gelangt, mittels verschiedener Sicherheitsfunktionen auf Bedrohungen hin untersucht. Die dazu eingesetzten und weiteren Funktionen sind nachfolgend beschrieben:

3.1.1 Intrusion Prevention System (IPS)

Der IPS Service bietet vollständige Funktionen zur Abwehr von Eindringlingen bei Multi-Gigabit-Übertragungsraten. Das IPS Service Blade sorgt mit vollständiger Intrusion-Prevention-Funktionalität für umfassenden Schutz vor böswilligem Datenverkehr im Netzwerk.

3.1.2 Application Control

Der Application Control Service bietet Praxen in jeder Größe ein hohes Maß an Anwendungssicherheit und Identitätskontrolle. Auf Grundlage von Benutzern oder Gruppen können granulare Richtlinien definiert werden und so die Nutzung von über 240.000 Web-2.0-Anwendungen und Widgets analysiert, gesperrt oder deren Nutzung beschränkt werden:

- UserCheck-Technologie informiert Mitarbeiter über Einschränkungen beim Anwendungszugriff und liefert gleichzeitig Informationen zu den Nutzungsrichtlinien des Unternehmens
- Erkennbarkeit artfremder Anwendungen über bekannte Ports: ssh über HTTPS (443)

3.1.3 URL-Filtering

Der URL-Filtering Service sorgt für eine übersichtliche, einheitliche Verwaltung und Durchsetzung von Aspekten der Websicherheit. URL-Filtering sorgt durch die vollständige Integration in das Gateway für optimale Websicherheit. Ein externer Proxy ist nicht erforderlich, da das System als Proxy arbeiten kann.

- Dynamische Cloud-basierte Datenbank mit über 100 Millionen Webseiten
- Keine Umgehung mit externen Proxys dank vollständiger Integration von URL-Filtering im Gateway

3.1.4 Anti-Bot

Der Anti-Bot Service wurde speziell entwickelt, um Bots im Netz zu enttarnen und zu stoppen. Diese Lösung basiert auf Check Points Multi-Tier ThreatSpect™ Technologie, die Unternehmen dabei hilft, Gefahren aufzudecken, abzuwenden und künftigen Angriffen vorzubeugen. Multi-Tier ThreatSpect™ ist eine einzigartige Detection-Engine, die den Datenverkehr auf jedem Gateway analysiert, Gefahrenausbrüche identifiziert und Bots aufdeckt, indem sie eine Vielzahl von Risikofaktoren miteinander korreliert – etwa Botnet-Muster und –Profile, die Verstecke entfernter Betreiber und die Verhaltensweisen von Attacken. Wurde ein Bot identifiziert, kann das Unternehmen über intuitive Dashboards schnell feststellen, welches Risiko für die Geschäftsabläufe besteht – etwa durch Datenverlust oder betrügerische Spam-Software

3.1.5 Anti-Virus

Zum Zwecke der umfassenden Gefahrenprävention kommt Check Points Anti-Virus Service zum Einsatz, welcher ebenfalls von der Threat Cloud mit Informationen versorgt wird. Diese Lösung ermöglicht es Unternehmen, den Zugriff auf Malware-infizierte Websites einzudämmen und Host-Systeme vor unbekannten Virus-Infektionen, die sich über das Netzwerk einschleichen, zu schützen. Über intuitive Dashboards können Bot- und Malware-Bedrohungen schnell analysiert und auftretende Gefahren, sowie deren Risiko-Level, herausgestellt werden und daraus resultierende Sicherheitsauswirkungen für das Unternehmen aufzeigen – wie zum Beispiel Datenverlust oder eine Zunahme an betrügerischem Spam-Aufkommen:

- aktuelle Datenbank auf Basis der Check Point Threat Cloud
- Anti-Virus auf bestehende Gateways

3.1.6 Anti-Spam

Der Check Point Anti-Spam und E-Mail Security Service bietet umfassenden Schutz für die E-Mail-Infrastruktur von Unternehmen, darunter auch akkuraten Spamschutz und Echtzeitschutz vor einer Vielzahl durch E-Mail verursachter Bedrohungen.

- Genaue Erkennung von Bedrohungen in Echtzeit
- Kontinuierliche Aktualisierungen bieten Echtzeitschutz vor Spam und Malware
- Vollständige Kontrolle der Endanwender, ohne dass eine Installation beim Endanwender notwendig ist
- Content- und Sprachunabhängig

3.2 TELEMED Protect Router

Mit dem TELEMED Protect Router stellt TELEMED einen gemanagten Router auf Basis von hochsicheren Produkten bereit (siehe auch Punkt 1.1). Der eingesetzte Router wird dabei, im Anschluss an die Erstinstallation, mittels Fernzugriff gewartet und administriert. Der für die Wartung genutzte Wartungstunnel (always on) ist dabei wie folgt spezifiziert:

- IKEv2-Tunnel mit zertifikatsbasierter Authentifizierung

TELEMED realisiert über diesen VPN-Tunnel die folgenden Dienste, soweit vereinbart:

- Wartungsarbeiten
- Mehrwertdienste
- Service- und Supportunterstützung

Zudem findet eine permanente Überwachung des Einwahlrouters statt, wodurch eine Alarmierung bei Auffälligkeiten, wie z. B. dem Ausfall der Internetverbindung, gewährleistet wird. Die Benachrichtigung über solche Ereignisse erfolgt an die vom Auftraggeber angegebene E-Mail-Adresse.

Die Routerkonfiguration wird, wie folgt, auf TELEMED-eigenen Servern gesichert, um eine schnelle Wiederherstellung im Supportfall zu ermöglichen:

- täglich
- wöchentlich
- monatlich

Dabei werden die Backups wie folgt vorgehalten:

- täglich = sieben Tage
- wöchentlich = vier Wochen
- monatlich = sechs Monate

Sämtliche Firmwareupdates werden durch TELEMED vor Einspielen in die Systeme des Auftraggebers qualitätsgesichert um Systemausfälle durch fehlerhafte Firmwarestände auszuschließen.

4. Investitionsversprechen

Das TELEMED Protect Platin Paket beinhaltet ein Investitionsversprechen, welches sich auf die in dieser Leistungsbeschreibung beschriebenen Paketbestandteile (Paketbestandteile) in der in der Leistungsbeschreibung benannten Konfiguration erstreckt. Das Investitionsversprechen hat folgenden Inhalt:

Sofern eine oder mehrere der Paketbestandteile nicht der von der KBV gemäß § 75b Abs. 1 SGB V bis zum 30.06.2020 festzulegenden Richtlinie zur Sicherheit der vertragsärztlichen und vertragszahnärztlichen Versorgung (Richtlinie) entsprechen, werden diese innerhalb von 6 Monaten nach Inkrafttreten der Richtline

kostenfrei von TELEMED an die Anforderungen der Richtlinie angepasst oder durch geeignete Bestandteile ersetzt. Die Implementierung dieser Änderungen und Anpassungen beim Auftraggeber erfolgen soweit möglich über Fernzugriffe.

Die aus dem Investitionsversprechen resultierenden Änderungen und Anpassungen der Paketbestandteile berechtigen nicht zur vorzeitigen Kündigung des Vertrags.

Aus dem Investitionsversprechen ergeben sich für den Auftraggeber keine Ansprüche auf Erweiterung des vereinbarten Leistungsumfangs oder auf den Bezug weiterer Leistungen sondern lediglich der Anspruch darauf, dass die in der Leistungsbeschreibung konkret benannten und mit dem Auftraggeber im jeweiligen Einzelfall vertraglich vereinbarten Paketbestandteile in ihrer jeweils vereinbarten Ausführung der zum 30.06.2020 zu erlassenden Richtlinie entsprechen bzw. nach Maßgabe dieses Investitionsversprechens soweit erforderlich hieran angepasst werden. Das Investitionsversprechen bezieht sich inhaltlich auch nicht auf etwaige weitere zukünftige Fortschreibungen der zum 30.06.2020 zu erlassenden Richtlinie, sondern ausschließlich auf die Anpassung der in der Leistungsbeschreibung benannten Paketbestandteile auf die Richtlinie in dieser Fassung.

5. Nachträgliche Änderungen

Nachträgliche Änderungen der Produktkonfigurationen sind ausschließlich im Rahmen des Geltungsbereiches der IT-Sicherheitsrichtlinie gemäß §75b SGB V möglich. Änderungen können z. B. dann notwendig sein, wenn neue Geräte in das Praxisnetzwerk implementiert werden sollen. Diese werden, soweit möglich, aus der Ferne durchgeführt und gemäß der jeweils gültigen TELEMED-Preisliste berechnet.

6. Service-Level-Agreement (SLA) für Protect Platin

6.1 Servicezeiten / Servicebereitschaft

Jegliche Art von Service- und Supportanliegen meldet der Auftraggeber unter Nennung aller erforderlichen Daten, insbesondere seiner Kundennummer grundsätzlich per Telefon, Fax oder E-Mail und sofern vorhanden über die dafür vorgesehenen Formulare, welche unter www.cgm.com/telmed-download zur Verfügung stehen. Die Annahme und Bearbeitung von Service- und Supportanliegen erfolgt werktags - ausgenommen samstags - in der Zeit zwischen 08:00 Uhr und 18:00 Uhr.

6.2 Reaktionszeiten für Protect Platin

Im Rahmen des Platin-Service reagiert TELEMED binnen zwei Stunden innerhalb der Servicezeiten ab Meldung des Service- oder Supportanliegens.

Meldungen, die nachts in der Zeit zwischen 18:00 Uhr und 08:00 Uhr, samstags, sonntags oder an gesetzlichen Feiertagen eingehen, beginnt die Reaktionszeit am folgenden Werktag um 08:00 Uhr. Fällt das Ende der Wiederherstellungsfrist auf einen Zeitpunkt zwischen 18:00 Uhr und 08:00 Uhr, auf einen Samstag, Sonntag oder gesetzlichen Feiertag, wird die Wiederherstellungsfrist ausgesetzt und am folgenden Werktag um 08:00 Uhr fortgesetzt.

6.3 Bearbeitungszeit für Protect Platin

TELEMED bearbeitet die Service- und Supportanliegen innerhalb von 24 Stunden während der angegebenen Servicebereitschaftszeiten. Die Bearbeitungszeit beginnt, mit Ablauf der Reaktionszeit, jedoch frühestens sobald alle erforderlichen Angaben durch den Auftraggeber gemacht wurden. Die Bearbeitungszeit wird während der Lieferzeiten und ggf. Reparaturen der eingesetzten Endgeräte ausgesetzt.

Muss ein Anliegen, auf ausdrücklichen Wunsch des Auftraggebers oder weil dies zur Bearbeitung erforderlich ist, am Standort des Auftraggebers bearbeitet werden, kann die Bearbeitung frühestens am darauffolgenden Werktag, ausgenommen samstags, erfolgen, sofern das Anliegen bis 10 Uhr gemeldet wurde.