

Leistungsbeschreibung CGM TELEMED Protect Gold

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 geschützt, vor Ausfällen und Bedrohungen aus dem Internet. Ziffer 4 beschreibt den Umgang mit nachträglichen Anpassungen auf Wunsch des Auftraggebers und unter 5 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 sind 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/telemmed-download eingesehen werden.

1.2 Anzahl der Endgeräte (PC-Arbeitsplätze oder Server)

Grundsätzlich können beliebig viele Endgeräte (PC-Arbeitsplätze oder Server) mit den TELEMED Protect Paketen geschützt werden. Das jeweils einzelne Paket umfasst den Schutz von bis zu fünf Endgeräten (PC-Arbeitsplätze oder Server).

1.3 Systemvoraussetzungen

Vom Auftraggeber zu stellende Voraussetzung für Installation und Nutzung der Produkte 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.

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)

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-Plattform (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 Endpoint 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 erkannte Schadsoftware registriert, da nach der Klassifizierung alle als unbekannt eingestuftes 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
- 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 Patch

TELEMED Protect Patch ist eine Patchmanagement Lösung, welche eine zentralisierte Echtzeit-Sicherheitsstatusübersicht für erkannte 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 einen monatlichen Managementbericht an eine bei Bestellung hinterlegte E-Mail Adresse.

2.4 TELEMED Protect Monitoring

Der TELEMED Protect Monitoring Dienst wird auf den Servern und Clients des Auftraggebers 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 2.4.1 definierte Auslastung erreicht, der PC ausfällt (siehe 2.4.3) oder TELEMED Protect Endpoint Pro deaktiviert wird (2.4.2), erfolgt automatisch eine Benachrichtigung per E-Mail an die vom Auftraggeber im Bestellschein angegebene E-Mail-Adresse.

Es gelten die unter 2.4.1 - 2.4.3 definierten Prüfintervalle und Grenzwerte:

2.4.1 Festplattenkapazität:

Intervall: 15 Minuten

Prüfobjekt: Festplatte C:

Prüfattribut: "Disk Free (GB)"

Benachrichtigung:

Warnmeldung bei ≥ 10 GB und < 20 GB freier Platz

Kritische Meldung bei < 10 GB freier Platz

2.4.2 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

2.4.3 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: >600 s

Benachrichtigungen werden nur für Serverbetriebssysteme verschickt, nicht für Workstations, da Workstations i. d. R. zum Feierabend abgeschaltet werden.

2.5 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:

- Adult Content
- Sex
- Dynamic DNS
- Elevated Exposure
- Emerging Exploits
- Suspicious Content
- Hacking
- Proxy Avoidance
- Unauthorized mobile Marketplaces
- Parked Domain
- Advanced Malware Command and Control
- Bot Networks
- Compromised Websites
- Keyloggers
- Malicious Embedded Link
- Malicious Embedded Iframe
- Malicious Websites
- Mobile Malware
- Phishing and other Frauds
- Potentially Unwanted Software
- Spyware

- Suspicious Embedded Link

Die Freischaltung der zuvor genannten Kategorien kann schriftlich beauftragt werden. Dabei gelten die Regelungen von Punkt 4 (Nachträgliche Änderungen) dieser Leistungsbeschreibung.

Gleiches gilt für die Aktivierung der nachfolgenden Funktionen, auf Wunsch des Auftraggebers:

- 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.

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

Bei der TELEMED Protect Firewall 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 setzt TELEMED eine Hardware-Firewall Lösung ein:

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.

Dabei werden sämtliche eingehenden sowie ausgehenden Verbindungen gesperrt und nur diejenigen Verbindungen, welche wirklich benötigt werden, geöffnet (Sparsamkeitsprinzip).

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)

Dieser Dienst überwacht mithilfe laufend aktualisierter Signaturen den Datenverkehr in allen gängigen Protokollen und bietet Echtzeit-Schutz vor Netzwerkbedrohungen.

3.1.2 Contentfilter

Der Contentfilter der TELEMED Protect Firewall entspricht in seiner Funktion und Konfiguration dem TELEMED Protect Contentfilter (siehe 2.5), jedoch gelten die Restriktionen für alle Geräte im Netzwerk und betreffen somit z. B. auch Smartphones und Tablets, welche per WLAN mit der Firewall oder einem dahinterliegenden Accesspoint verbunden sind.

3.1.2 Application Control

Mit diesem Feature können Sie den Zugriff auf Anwendungen in Abhängigkeit von Abteilung, Position im Unternehmen und Tageszeit gewähren, verweigern oder einschränken. Anschließend verfolgen Sie in Echtzeit, was von wem aufgerufen wurde.

3.1.3 WebBlocker-URL-Filterung

Blockiert bösartige Websites automatisch; durch Einsatz granularer Content-Filter-Tools können unangemessene Inhalte blockiert und die Produktivität gesteigert werden.

3.1.4 Reputation Enabled Defense (RED)

Reputation Enabled Defense (RED) Ein cloudbasierter Reputations-Suchdienst, der Benutzer vor bösartigen Websites und Botnets schützt und dabei den Overhead bei der Webverarbeitung erheblich verbessert.

3.1.5 Anti-Virus

Laufend aktualisierte Signaturen identifizieren und blockieren bekannte Spyware, Viren, Trojaner und mehr – einschließlich neuer Varianten bekannter Viren.

3.1.6 Threat Detection and Response

Threat Detection and Response setzt Sicherheitsereignisse im Netzwerk und am Endpunkt in Bedrohungsanalysen in Beziehung. Dadurch können potenzielle Angriffe noch früher erkannt, priorisiert und bewertet werden. Sofortmaßnahmen zur Abwehr erfolgen ohne Verzögerung.

3.1.7 DNSWatch

Verringert Infektionen durch Schadsoftware, indem bösartige DNS-Anforderungen blockiert und Benutzer zu Informationen umgeleitet werden, die ihnen Best Practices in puncto Sicherheit vermitteln und betonen, wie wichtig deren Einhaltung ist.

4. Nachträgliche Änderungen

Nachträgliche Änderungen der Produktkonfiguration müssen schriftlich beauftragt werden. Dabei obliegt es dem Auftraggeber zu prüfen, ob die Änderung im Einklang mit der IT-Sicherheitsrichtlinie nach §75b SGB V (Richtlinie) stattfindet. Die Bestandteile der TELEMED Protect Pakete sind so konfiguriert, dass diese im Einklang mit der Richtlinie stehen. Änderungen der Produktkonfiguration können dazu führen, dass der geänderte Paketbestandteil nicht mehr der Richtlinie entspricht. Mit Beauftragung der Konfigurationsänderung durch den Auftraggeber geht TELEMED davon aus, dass dieser die Richtlinienkonformität geprüft hat und evtl. aus der Freischaltung resultierende Risiken für die IT-Sicherheit bewusst akzeptiert.

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.

5. Service-Level-Agreement (SLA) für Protect Gold

5.1 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/telemmed-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.

5.2 Reaktionszeiten für Protect Gold

Im Rahmen des Gold-Service reagiert TELEMED binnen vier 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.

5.3 Bearbeitungszeit für Protect Gold

TELEMED bearbeitet die Service- und Supportanliegen innerhalb von 48 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.