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 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.

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

Die TELEMED Protect Firewall wird im Einwahlrouter oder als separates Gerät direkt dahinter, dem gesamten Praxisnetzwerk vorgeschaltet. Es handelt sich dabei um eine sogenannte Stateful Inspection Firewall, welche über von TELEMED definierte Regeln den Datenverkehr der Praxis eingehend und ausgehend reguliert.

Für einen maximalen Schutz und bestmögliche Kontrolle über den Datenverkehr wird im Rahmen der Installation zunächst jeglicher Datentransfer durch die Firewall unterbunden, um danach selektiv die benötigten Funktionen und Kommunikationspfade freizuschalten. Dies bietet z.B. Schutz vor sog. "Trojanern" bzw. E-Mail-Viren, die aktiv eine ausgehende Verbindung über bestimmte Ports aufbauen.
TELEMED setzt dabei auf die "Deny-All-Regel" zum Schutz des lokalen Netzwerks. Mit dieser Regel verfährt die Firewall nach dem Prinzip: “Alles, was nicht ausdrücklich erlaubt ist, bleibt verboten.” Damit wird ausgeschlossen, dass versehentlich vergessen wird bestimmte Einfallstore in die Praxis zu schließen. Im Rahmen der technischen Vorqualifikation mit dem Auftraggeber sowie der Installation werden die benötigten Freigaben erfasst und konfiguriert. Hierbei kann es ggfs. zu Einschränkungen durch die IT-Sicherheitsrichtlinie gemäß §75b SGB V kommen.
Wichtig: Die Grenzen einer Stateful-Inspection-Firewall sind durch die erlaubten Verbindungen bedingt, da diese nicht untersucht werden. Werden z. B. die Ports für die E-Mail-Kommunikation bewusst geöffnet, kann durchaus Schadsoftware via E-Mail in die Praxis gelangen.

3.2 TELEMED Protect Router Pro

Mit dem TELEMED Protect Router Pro stellt TELEMED einen gemanagten Router auf Basis von hochsicheren LANCOM-Produkten bereit. Der eingesetzte Router wird dabei, im Anschluss an die Erstinstallation, aus der Ferne gewartet und administriert.
Der für etwaig erforderliche Zugriffe genutzte Wartungstunnel (always on) ist dabei wie folgt spezifiziert:

- IKEv2-Tunnel mit zertifikatsbasierter Authentifizierung

TELEMED realisiert über diesen VPN-Tunnel die folgenden, ggfs. zusätzlich vereinbarten Dienste:

- Wartungsarbeiten
- Mehrwertdienste
- Service- und Supportunterstützung

Zudem findet automatisiert 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:

- tägliche = sieben Tage
- wöchentliche = vier Wochen
- monatliche = sechs Monate

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

Zudem wird durch die Nutzung des TELEMED Protect Router Pro sämtlicher Internet-Datenverkehr des Auftraggebers, mit Ausnahme der Telefonie-Daten, mittels eines verschlüsselten Tunnels über das sichere TELEMED Rechenzentrum ins Internet geleitet, damit Identität und Internetaktivitäten des Auftraggebers verborgen und geschützt bleiben. TELEMED überwacht dabei mittels eines zentralen Virenschutzes den unverschlüsselten Datenstrom und leitet zusätzlich jeglichen Datenstrom über eine zentrale Firewall.

4. 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.

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/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.

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.