Leistungsbeschreibung CGM TELEMED Protect Silber

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. Ziffer 3 beschreibt den Umgang mit nachträglichen Anpassungen auf Wunsch des Auftraggebers.

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/telemed-download eingesehen werden.

1.2 Anzahl der PC-Arbeitsplätze

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 zur 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-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 erkannte 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
- 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 Dienst wird auf Arbeitsplätzen und Servern 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 >= 10GB und < 20GB freier Platz
Kritische Meldung bei < 10GB 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 : >600s
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 3 (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. 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.