Leistungsbeschreibung CGM TELEMED Protect Firewall Pro

(auf Basis Check Point CP730)

1. Einleitung

Die CompuGroup Medical Deutschland AG Geschäftsbereich TELEMED (im Folgenden TELEMED genannt) bietet dem Auftraggeber einen Managed Firewall Service, inkl. der dafür benötigten Hardware an. Der Firewall-Service regelt dabei die Kommunikationsbeziehungen zwischen dem Netzwerk des Auftraggebers und dem Internet, hinsichtlich der Zugriffsmöglichkeiten aus dem und in das Netzwerk des Auftraggebers. Grundlage hierfür ist die von TELEMED definierte Grundkonfiguration (siehe 6.2), sowie die vom Auftraggeber beauftragten individuellen Regeln, gemäß Vertragsanlage "TELEMED Protect Firewall Pro - Regeln".
Der Umfang der insgesamt vertraglich vereinbarten Leistungen ergibt sich aus dieser Leistungsbeschreibung und ggfs. weiteren Leistungsbeschreibungen der vom Auftraggeber bestellten Leistungen sowie aus den Allgemeinen Geschäftsbedingungen der TELEMED und den Besonderen Geschäftsbedingungen für die CGM TELEMED Protect Firewall Pro.

2. Zuständigkeiten

Bei Erteilung des Auftrags wird definiert, wer zukünftig Ansprechpartner für den Auftraggeber ist. Dabei wird zwischen TELEMED und einem von TELEMED zertifizierten Vertriebs- und Servicepartner unterschieden. Es ist zu beachten, dass hierdurch Unterschiede in den Preislisten entstehen können. Gültig ist jeweils die aktuelle Preisliste des im Auftrag definierten Ansprechpartners. TELEMED behält sich zudem das Recht vor, externe Dienstleister mit Service und Support zu beauftragen. Diese sind an die jeweils gültige Fassung der TELEMED Preisliste gebunden.

3. Funktionsumfang der Firewall

3.1 VPN (IPsec)

Die IPsec VPN-Software integriert Zugriffskontrolle, Authentifizierung und Verschlüsselung, um eine sichere Verbindung zu Unternehmensnetzwerken für Remote- und mobile Benutzer, Zweigstellen und Geschäftspartner über das Internet zu gewährleisten.

3.2 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.

3.3 Application Control

Der Application Control Service bietet Unternehmen in jeder Größe ein Höchstmaß 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
- Analyse von SSL-verschlüsseltem Datenverkehr[1]
- Erkennbarkeit artfremder Anwendungen über bekannte Ports: ssh über HTTPS (443)

3.4 URL-Filtering

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

- Dynamische Cloud-basierte Datenbank mit über 100 Millionen Webseiten

[1] Wichtige Informationen zur SSL-Inspection können den Besonderen Geschäftsbedingungen der TELEMED Protect Firewall Pro entnommen werden.

- Keine Umgehung mit externen Proxys dank vollständiger Integration von URL-Filtering in Check Point Gateways
- Prüfung SSL-verschlüsselten Datenverkehrs im Gateway bei Bedarf

3.5 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

3.6 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:

- Jederzeit aktuelle Datenbank auf Basis der Check Point Threat Cloud, die mehr als 300-mal so viele Signaturen enthält als frühere Versionen
- Anti-Virus auf bestehende Gateways

3.7 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.

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

3.8 Sandblast Threat Emulation

Der Check Point Threat Emulation Service beugt Infektionen durch unbekannte Exploits, Zero-Day oder gezielten Angriffen vor. Diese Lösung inspiziert verdächtige Dateien sowie deren Funktionalitäten auf kundeneignen Appliances oder in der Cloud und verhindert so, dass diese in das Netzwerk eindringen. Aufgespürte Malware kommuniziert die Threat Emulation an die Check Point Threat Cloud. Um den hohen Ansprüchen an die Datensicherheit im Gesundheitswesen gerecht zu werden, nutzt CGM / TELEMED eine eigene Threat Cloud. Die Daten des Auftraggebers werden somit nicht in der Cloud von Check Point, sondern im eigenen Rechenzentrum in Deutschland inspiziert. Zudem werden die Ergebnisse der Analysen nicht an Check Point weitergegeben. Die CGM / TELEMED-eigene Threat Cloud wird jedoch von Check Point regelmäßig mit Analysedaten versorgt um einen effektiven und effizienten Schutz des Netzwerks des Auftraggebers zu gewährleisten.

3.9 SSL-Inspection

Die SSL-Inspection ermöglicht es, verschlüsselte Verbindungen aufzubrechen, um darüber übertragene Inhalte auf Malware zu untersuchen. Zu diesem Zweck, wird ein Man-in-the-Middle Verfahren eingesetzt, welches voraussetzt, dass auf allen Geräten des Auftraggebers, welche mit dem Internet kommunizieren, ein eigens von der Firewall ausgestelltes Sicherheitszertifikat installiert wird. Möchte der Auftraggeber, nach erfolgter Inbetriebnahme der TELEMED Protect Firewall Pro, weitere Geräte in sein Netzwerk einbinden, kann es notwendig sein, dass TELEMED, oder ein von TELEMED zertifizierter Vertriebs- und Servicepartner, Konfigurationsänderungen vornehmen und / oder das Sicherheitszertifikat auf

diesen Geräten installieren muss. Die Kosten hierfür sind vom Auftraggeber zu tragen. Weitere Informationen zur SSL-Inspection können den Besonderen Geschäftsbedingungen entnommen werden.

4. Nutzung von TELEMED Mehrwertdiensten

Bestandteil der TELEMED Protect Firewall Pro ist ein sicherer VPN-Tunnel (IPsec) in das TELEMED-Rechenzentrum. Dieser ermöglicht dem Auftraggeber die Nutzung zusätzlicher CGM bzw. TELEMED Mehrwertdienste, wie z. B. DALE-UV und Bonitätsprüfung. Die Nutzung der einzelnen Mehrwertdienste unterliegt den jeweiligen Leistungsbeschreibungen und ggfs. Besonderen Geschäftsbedingungen. Zudem müssen die Dienste separat beauftragt werden und es können Kosten, gemäß der jeweils gültigen Preisliste, entstehen. Für die Einrichtung des VPN-Tunnels ist ggfs. die Installation einer Software auf den Clients des Auftraggebers notwendig. Sollte die Installation der Software nicht im Rahmen der Basisinstallation (siehe Punkt 5.1) abbildbar sein, kann eine kostenpflichtige individuelle Konfiguration erforderlich sein.

5. Bereitstellung: Installation und Policy-Konfiguration

5.1 Basisinstallation

Die Basisinstallation findet nach Absprache Werktags zwischen 8 und 18 Uhr statt. Außerhalb dieses Zeitfensters wird ein Aufschlag berechnet. Der Installationstermin muss dabei, seitens des Auftraggebers, so gewählt / abgestimmt werden, dass der ausführende Techniker seine Tätigkeiten unterbrechungsfrei durchführen kann. Eine Garantie für die Umsetzung von Terminwünschen kann nicht zugesprochen werden, allerdings ist TELEMED stets bemüht, auf die Wünsche des Auftraggebers einzugehen. Im Vorfeld der Installation wird es ggfs. zu einer Kontaktaufnahme durch den Installationsdienstleister kommen, um eine Vorqualifikation mit dem Auftraggeber durchzuführen. Diese dient dem Zweck, den Betriebsablauf, am Tag der eigentlichen Installation, möglichst wenig zu stören, indem, mittels der, durch den Auftraggeber, bekanntgegebenen Informationen eine Vorkonfigurierung der Hardware erfolgt. Bestandteile der Basisinstallation sind die Anfahrt innerhalb des deutschen Festlands, sowie Einbindung und Inbetriebnahme der Firewall in das Netzwerk des Auftraggebers. Anschließend wird eine Grundkonfiguration, sowie das Installieren der notwendigen Sicherheitszertifikate durchgeführt. Um diese Sicherheitszertifikate einspielen zu können, muss dem Techniker Zugang zu den Clients gewährt werden. Für den Fall, dass es dabei zu, durch den Auftraggeber verschuldeten, Verzögerungen kommt, behält TELEMED, bzw. der zertifizierte Vertriebs- und Servicepartner, sich das Recht vor, die Mehraufwände gemäß Preisliste zu fakturieren. Die Einrichtung der Firewall als Einwahlrouter für den Online-Zugang ist nicht Bestandteil. Seitens des Auftraggebers muss sichergestellt sein, dass die Voraussetzungen für den Betrieb der Firewall erfüllt sind (siehe Besondere Geschäftsbedingungen zur TELEMED Protect Firewall Pro). Für die Basisinstallation steht ein vordefiniertes Zeitkontingent zur Verfügung, welches dem jeweils zugrundeliegenden Teilnahmeantrag zu entnehmen ist. Ist dies nicht der Fall behält TELEMED bzw. der zertifizierte Vertriebs- und Servicepartner sich das Recht vor, die Installation abzubrechen und in Rechnung zu stellen. Nach erfolgter Einrichtung wird stichprobenartig eine Kontrolle der Firewall-Policy durchgeführt.

5.2 Grundkonfiguration

Alle Sicherheitsfeatures der Firewall (siehe Punkt 3) sind standardmäßig aktiviert. Hiervon ausgenommen ist die SSL-Inspection, welche nur nach ausdrücklicher Zustimmung des Auftraggebers aktiviert wird[1]. Ausgehende Verbindungen, aus dem Netzwerk des Auftraggebers, werden zugelassen, eingehende Verbindungen jedoch blockiert. Ausnahme stellen eingehende Verbindungen dar, welche von Produkten der CompuGroup Medical Deutschland AG benötigt werden. Eingehende Verbindungen für Fremdsoft- und Hardware können durch eine individuelle Konfiguration ermöglicht werden (siehe Punkt 5.4). Über einen Content-Filter wird der Zugriff auf Seiten mit Hacking -Inhalten beschränkt. Weitere Filter können im Rahmen der Basisinstallation, oder durch nachträgliche Konfigurationsänderungen, individuell aktiviert werden, je nach Wunsch des Auftraggebers.

[1] Wichtige Informationen zur SSL-Inspection können den Besonderen Geschäftsbedingungen der TELEMED Protect Firewall Pro entnommen werden.

5.3 Individuelle Konfiguration

Basierend auf einer, vom Auftraggeber erstellten, Firewall-Policy, kann, im Rahmen der Basisinstallation, eine weitergehende, individuelle Konfiguration erfolgen. Sofern, zwecks Vorqualifizierung, eine telefonische Kontaktaufnahme durch einen Installationsdienstleister, oder zertifizierten Vertriebs- und Servicepartner, erfolgt, hat der Auftraggeber diesen über die individuellen Regeln in Kenntnis zu setzen, um den Aufwand am Tag der Installation möglichst gering zu halten. Die Individuelle Konfiguration wird, sofern Sie nicht im Rahmen der Leistungen, gemäß Punkt 6.1 dieser Leistungsbeschreibung, abbildbar ist, anhand der jeweils gültigen Preisliste in Rechnung gestellt.

Individuelle Konfigurationen, welche nicht im Rahmen der Basisinstallation stattfinden, gelten als Standard Konfigurationsänderungen (siehe Punkt 6.1).

5.4 Mitwirkungspflichten des Kunden

Im Anschluss an die Inbetriebnahme der Firewall erhält der Auftraggeber ein Installationsprotokoll. Mit seiner Unterschrift auf diesem Protokoll, bestätigt der Auftraggeber, dass alle individuellen Regeln auf Funktion geprüft wurden. Gleiches gilt auch für Geräte und Dienste, welche bereits vor der Installation durch den Auftraggeber genutzt wurden. Wird eine Einschränkung erst zu einem späteren Zeitpunkt festgestellt, so hat der Auftraggeber kein Recht auf Nachbesserung vor Ort. Die Nachbesserung erfolgt im Rahmen des, im Teilnahmeantrag definierten, Remote-Services. TELEMED behält sich vor, Mehraufwände, welche auf eine nicht ausreichende Funktionsprüfung, seitens des Auftraggebers, zurückzuführen sind, gemäß Preisliste in Rechnung zu stellen.

6. Änderungen der Firewall-Policy

6.1 Standard Konfigurationsänderung

Konfigurationsänderungen müssen schriftlich mit der Anlage "TELEMED Protect Firewall Pro - Regeln" bekannt gegeben werden und werden nur akzeptiert sofern Sie von vertretungsberechtigten Personen unterzeichnet wurden. Diese werden binnen 48 Stunden, innerhalb der Servicebereitschaftszeiten, gemäß Punkt 8.2 dieser Leistungsbeschreibung, ab Auftragseingang durch TELEMED bzw. einen zertifizierten Vertriebs- und Servicepartner bearbeitet. Sind die erforderlichen Angaben auf dem Änderungsauftrag unvollständig, berechnet TELEMED, oder der zertifizierte Vertriebs- und Servicepartner, den Mehraufwand gemäß Preisliste.

6.2 CGM eigene Systeme

Erlangt TELEMED Kenntnis darüber, dass, z. B. auf Grund von Updates / Upgrades von CGM Software, wie Arzt- bzw. Zahnarztinformationssystemen, Änderungen der Konfiguration notwendig werden, so wird TELEMED diese Konfigurationsänderungen für den Auftraggeber kostenfrei und automatisiert einspielen. Die Konfigurationsänderungen erfolgen grundsätzlich aus der Ferne und werden nicht vor Ort, beim Auftraggeber, durchgeführt. TELEMED übernimmt keine Garantie dafür, dass notwendige Anpassungen bereits bei der Auslieferung von CGM-Softwareupdates zur Verfügung stehen.

7. Reportings

Der Auftraggeber erhält einen monatlichen Report über die Aktivitäten seiner Firewall. Dieser Report wird an die, vom Auftraggeber auf dem Teilnahmeantrag festgelegte, E-Mail-Adresse versandt.

8. Service-Level-Agreement (SLA)

Die Meldung und Bearbeitung von Servicebeeinträchtigungen erfolgt über den im Auftrag definierten Ansprechpartner. Beachten Sie, dass der von TELEMED zertifizierte Vertriebs- und Servicepartner ggfs. abweichende Zeiten für die Servicebereitschaft und Servicewiederherstellung benennt.

8.1 Definition von Servicebeeinträchtigungen im Rahmen der Protect Firewall Pro Services

Eine Servicebeeinträchtigungen liegt immer dann vor, wenn die Firewall als Ganzes ausfällt, oder einzelne Leistungsmerkmale trotz korrekter Konfiguration / Installation nicht mehr funktionieren. Beeinträchtigungen, die im Zusammenhang mit der Firewall-Policy auftreten, wie z. B. die Nicht-Erreichbarkeit einer bestimmten Homepage / Applikation, oder neue Hardware im Kundennetzwerk, die nicht richtig mit dem Internet kommunizieren kann, gelten nicht als Servicebeeinträchtigungen und können gemäß dem Punkt **Änderungen der Firewall-Policy** dieser Leistungsbeschreibung behoben werden.

8.2 Meldung von Servicebeeinträchtigungen und Servicebereitschaft

Servicebeeinträchtigungen meldet der Auftraggeber unter Nennung aller zur Servicewiederherstellung erforderlichen Daten, insbesondere seiner Kundennummer grundsätzlich per Telefon, Fax oder E-Mail. Um eine schnelle Diagnose sicherzustellen, ist der Auftraggeber angehalten, die Symptome der Servicebeeinträchtigungen möglichst genau zu beschreiben. Liegen TELEMED alle notwendigen Informationen vor, beginnt die Wiederherstellung des Services. Die Bearbeitung von Servicebeeinträchtigungen durch die Servicebereitschaft erfolgt werktags - ausgenommen samstags - in der Zeit zwischen 08:00 Uhr und 18:00 Uhr. Meldungen von Servicebeeinträchtigungen, die nachts in der Zeit zwischen 18:00 Uhr und 08:00 Uhr, samstags, sonntags oder an gesetzlichen Feiertagen eingehen, beginnt die Wiederherstellungsfrist 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.

8.3 Servicebeeinträchtigung und -wiederherstellung

TELEMED beseitigt Servicebeeinträchtigungen, welche im Einflussbereich von TELEMED liegen, innerhalb von 24 Stunden während der angegebenen Servicebereitschaftszeiten. Die Wiederherstellungszeit beginnt, ab Meldung durch den Auftraggeber und gilt als eingehalten, wenn der Service nach dieser Zeit wieder vollständig zur Verfügung steht. Die Wiederherstellungszeit wird während der Reparatur und ggf. Austausch der eingesetzten Endgeräte ausgesetzt, unabhängig davon ob diese von TELEMED, oder einem zertifizierten Vertriebs- und Servicepartner bezogen wurde. Ebenso wird die Wiederherstellungszeit ausgesetzt, bis alle, vom Auftraggeber geschuldeten, Informationen zu der Servicebeeinträchtigung vorliegen. Beeinträchtigungen, welche durch Updates / Neuanschaffungen, von Auftraggeber eigener Hard- und Software auftreten, stellen keine Servicebeeinträchtigung, im Sinne dieser Leistungsbeschreibung dar, da diese nicht im Einflussbereich von TELEMED liegen. In diesen Fällen muss der Auftraggeber TELEMED eine Standardkonfigurationsänderung, gemäß Punkt 6.1, mitteilen.

8.4 Kosten

Für die Servicewiederherstellung, sowie den ggfs. notwendigen Tausch von, durch TELEMED bezogener, Hardware, im Rahmen der Gewährleistung, entstehen dem Kunden keine Kosten, es sei denn, im Verlauf der Servicewiederherstellung wird festgestellt, dass die Servicebeeinträchtigung durch den Kunden verschuldet ist, oder dass gar keine Servicebeeinträchtigungen vorliegt. In diesen Fällen ist TELEMED oder der von TELEMED zertifizierte Vertriebs- und Servicepartner dazu berechtigt, den Aufwand gemäß der jeweils gültigen Preisliste in Rechnung zu stellen.

8.5 Erbringung kostenloser Leistungen

Eine derzeitige oder zukünftige, kostenlose Erbringung von Leistungen durch die TELEMED, oder von TELEMED zertifizierten Vertriebs- und Servicepartnern gegenüber dem Auftraggeber begründet keinen Erfüllungsanspruch. TELEMED kann derartige vergütungsfrei zur Verfügung gestellten Leistungen künftig auch gegen Entgelt anbieten. In einem solchen Fall wird TELEMED den Auftraggeber unverzüglich informieren.

8.6 Wartungsarbeiten

Wartungsarbeiten können zu einer geplanten Unterbrechung der Dienste führen und werden dem Kunden rechtzeitig bekannt gegeben. In dringenden Fällen kann eine außerplanmäßige Wartung erforderlich sein, ohne den Kunden vorzeitig zu informieren.