Besondere Geschäftsbedingungen CGM TELEMED Managed Firewall

1. Untersuchung verschlüsselter Datenverbindungen

Sofern vom Auftraggeber gewünscht aktiviert TELEMED die sogenannte SSL-Inspection. Mittels dieser werden verschlüsselte Verbindungen aufgebrochen, sodass auch deren Datenpakete auf etwaige Bedrohungen hin untersucht werden können. Die SSL-Inspection kann lediglich aktiviert oder deaktiviert werden, d. h. ist diese aktiviert besteht keine Möglichkeit zu differenzieren, welche Verbindungen mit welchen Websites entschlüsselt werden sollen und welche nicht. Es können allerdings einzelne Clients des Auftraggebers von der SSL-Inspection ausgeschlossen werden. Für alle Clients, welche an der SSL-Inspection teilnehmen, bedeutet dies, dass auch die private Internetnutzung, unabhängig davon ob diese vom Auftraggeber gestattet wurde, durch diesen Mechanismus aufgebrochen und analysiert wird. Aus diesem Grund empfiehlt TELEMED dem Auftraggeber, sämtliche Mitbenutzer der, durch die Firewall geleiteten Internetverbindung, darüber in Kenntnis zu setzen und sich eine schriftliche Einwilligung einzuholen.

Zum jetzigen Zeitpunkt betrifft dieses Vorgehen sämtlichen Datenverkehr mit https-Websites, sowie E-Mails, welche das Protokoll IMAPS nutzen. Die ebenfalls gängigen E-Mail-Protokolle POP3S und SMTPS werden folgen. TELEMED weißt explizit darauf hin, dass ein optimaler Schutz des Netzwerks nur dann erreicht werden kann, wenn der verschlüsselte Datenverkehr überprüft werden darf.

2. Deaktivierung der SSL-Inspection

TELEMED weißt explizit darauf hin, dass die Deaktivierung, bzw. Nichtaktivierung, der SSL-Inspection zu einem deutlich erhöhten Risiko für Schadsoftware (Malware) im Netzwerk des Auftraggebers führt. Dies ist dadurch bedingt, dass der Großteil des Datenverkehrs beim Surfen und der E-Mail-Korrespondenz heutzutage über verschlüsselte Protokolle abgewickelt wird. Ohne SSL-Inspection kann keine Untersuchung des verschlüsselten Datenverkehrs stattfinden und somit kann schadhafte Software über diese Wege in das Netzwerk des Auftraggebers gelangen. Dies gilt auch, wenn lediglich einzelne Clients der SSL-Inspection unterliegen, da sich über Clients ohne SSL-Inspection Schadsoftware im gesamten Netzwerk verbreiten kann.

3. Aktivierung der SSL-Inspection

Wünscht der Auftraggeber, bei Erstbeauftragung der CGM TELEMED Managed Firewall oder nachträglich, die Aktivierung der SSL-Inspection, geht TELEMED davon aus, dass dieser die, von TELEMED geschuldeten Leistungen, gemäß Vertrag und Vertragsanlagen, lediglich für seine eigenen Zwecke, bzw. die seines Geschäftsbetriebs, nutzt und / oder durch Dritte nutzen lässt. Ferner geht TELEMED davon aus, dass der Auftraggeber, für den abweichenden Fall, z. B. der privaten Nutzung durch Dritte, vor Freigabe der Dienste an Dritte, deren ausdrückliches Einverständnis zur Überprüfung des verschlüsselten Datenverkehrs eingeholt hat.

4. White-List für die SSL-Inspection

Manche Verbindungen, auf welche der Auftraggeber angewiesen ist, können bei aktivierter SSL-Inspection zu sporadischen / dauerhaften Fehlern beim Verbindungsaufbau mit dem angesprochenen Server führen. Dies

ist beispielsweise oftmals bei Laboranbindungen der Fall, da die Labore häufige veraltete, oder eigens ausgestellte Sicherheitszertifikate verwenden. Aus diesem Grund kann TELEMED, auf Basis der URL-Adresse, Ausnahmen für die SSL-Inspection generieren. Zwecks Reduzierung des Arbeitsaufwands und somit der Kosten für den Auftraggeber, stellt TELEMED eine White-List bereit, mit Ausnahmen für die SSL-Inspection. Auf dieser White-List befinden sich ausschließlich, von TELEMED für sicher befundene, Verbindungen, welche ohne eine solche Ausnahme zu technischen Schwierigkeiten führen können. Eine vollständige, aktuelle Liste, aller Ausnahmen, ist jederzeit im Download-Bereich, auf www.telemed.de, abrufbar.

5. HTTP Public Key Pinning (HKHP)

Einige https-Websites verwenden HKHP. Dies hat, in Abhängigkeit von dem verwendeten Browser, zur Folge, dass bei aktivierter SSL-Inspection Probleme mit dem Aufruf der Websites auftreten. Der erstmalige Aufruf der Website wird problemlos funktionieren, auf Grund des Trust On First Use Verfahrens. Wird die Website ein weiteres Mal besucht, blockiert der Browser den Zugriff darauf.

6. Voraussetzungen für den Betrieb

6.1 Internetverbindung

Für den Betrieb der CGM TELEMED Managed Firewall wird ein breitbandiger Internetanschluss vorausgesetzt, welcher spätestens am Tag der Installation zur Verfügung stehen muss. Auf Grund der hohen Qualitätskriterien, sowie des umfangreichen Supports wird ein All-IP Anschluss von TELEMED empfohlen, welcher zudem eine zusätzliche Absicherung des Online-Zugangs bietet. Es können aber auch breitbandige Internetanschlüsse anderer Provider gewählt werden. Unabhängig vom Provider muss sichergestellt sein, dass am Tag der Installation das Passwort des Einwahlrouters vorliegt. Soll die Firewall zeitgleich auch als Einwahlrouter genutzt werden, besteht zudem die Notwendigkeit, dass die Zugangsdaten des Internetanschlusses ebenfalls vorhanden sind.

6.2 Sichere Aufbewahrung

Da es sich bei der CGM TELEMED Managed Firewall um ein Sicherheitsprodukt handelt sollte das Endgerät gegen eine Manipulation vor Ort geschützt werden. Daher empfehlen wir das Gerät an einem sicheren Ort aufzubewahren. Zu diesem Zweck können z. B. zutrittsgesicherte Räume oder ein verschließbarer Serverschrank genutzt werden. Besteht auf Grund der Netzwerkstruktur nicht die Möglichkeit dazu, kann bei TELEMED ein, für diesen Zweck geeigneter, Wandverteiler geordert werden (gemäß Preisliste).

7. Nutzung von Wireless LANs in Verbindung mit der SSL-Inspection

Wünscht der Auftraggeber, im Rahmen der Erstinstallation oder nachträglich, neben der SSL-Inspection, die Aktivierung der Wireless LAN Funktion der Firewall, hat dieser zu beachten, dass die SSL-Inspection die verschlüsselten Verbindungen sämtlicher angebundener Geräte untersucht. Dies gilt sowohl für seine eigenen, als auch für die von Dritten. Ebenfalls ist dies der Fall, wenn hinter der Firewall irgendeine Form von WLAN-AccessPoint betrieben wird. TELEMED weißt explizit darauf hin, dass durch die Nutzung von Wireless LAN der Kreis der nutzenden Dritten ggfs. deutlich größer ausfällt und beispielsweise auch Kunden / Patienten / Mandanten des Auftraggebers darunterfallen. TELEMED geht auch hier davon aus, dass, wie unter Punkt 3 beschrieben, alle Dritten ihr

ausdrückliches Einverständnis zur Untersuchung des verschlüsselten Datenverkehrs gegeben haben, bevor ihnen Zugang zum Netzwerk und der damit verbunden Internetverbindung gewährt wird.

8. Zugangsdaten und Passwörter

Um die CGM TELEMED Managed Firewall vor Manipulation zu schützen, stellt TELEMED dem Auftraggeber keinerlei Passwörter und Zugangsdaten bereit. Nur so kann sichergestellt werden, dass diese nicht genutzt werden um bewusst, oder unbewusst, das Sicherheitsniveau zu verändern. Sämtliche Änderungen an den Einstellungen, werden von TELEMED oder einem von TELEMED geschulten und zertifizierten Vertriebs- und Servicepartner durchgeführt. Erfolgt die Betreuung des Auftraggebers durch einen geschulten und zertifizierten Vertriebs- und Servicepartner, so stellt TELEMED diesem alle benötigten Zugangsdaten und Passwörter bereit.

9. Änderungen der Konfiguration durch den Auftraggeber

Einstellungen an der Firewall dürfen nur von TELEMED und von TELEMED geschulten und zertifizierten Vertriebs- und Servicepartner durchgeführt werden. Hierfür gilt der Konfigurationsänderungsprozess gemäß Leistungsbeschreibung, sowie die dazugehörige Preisliste. TELEMED übernimmt keine Haftung für Schäden, die durch unberechtigte und unsachgemäße Änderungen an den Einstellungen der Firewall entstehen.

10. Nutzung anderer Einwahlrouter

Sofern im Netzwerk des Auftraggebers ein anderer Einwahlrouter, als die Firewall selbst, genutzt wird, oder zukünftig genutzt werden soll, wird dieser der Firewall vorgeschaltet. Bei der Installation durch TELEMED, oder durch einen von TELEMED geschulten und zertifizierten Vertriebs- und Servicepartner wird lediglich die Firewall selbst an diesem Einwahlrouter angeschlossen. Alle weiteren Netzwerkkomponenten werden, direkt oder über einen Switch, mit der Firewall verbunden, um sicherzustellen, dass auch wirklich der gesamte Datenverkehr durch diese geleitet wird. Der Auftraggeber muss sicherstellen, dass auch nach erfolgter Installation keine Netzwerkgeräte direkt am Einwahlrouter angeschlossen werden, da so der Schutz durch die Firewall umgangen und ggfs. das gesamte Netzwerk infiltriert werden kann. Wird ein Wireless-LAN-fähiger Einwahlrouter der Firewall vorgeschaltet, so muss die WLAN-Funktion deaktiviert werden, da sonst ebenfalls eine Umgehung der Schutzmechanismen der Firewall möglich ist. Für Schäden, die durch eigenmächtige Änderung dieser Konstellation entstehen, übernimmt TELEMED keinerlei Haftung.

11. Schutz des Endpunktes

TELEMED stellt mit der CGM TELEMED Managed Firewall einen sehr hohen Schutz gegen Bedrohungen aus dem Internet bereit. Dennoch weißt TELEMED hiermit explizit darauf hin, dass die CGM TELEMED Managed Firewall nicht den lokalen Schutz der Clients, durch eine Anti-Virus-Software, ersetzt, da schadhafte Software nicht zwingend ausschließlich über das Internet verbreitet wird, sondern auch über lokale Datenträger, wie USB-Sticks, Smartphones etc.

12. Sicherheit der Daten

Zur Gewährleistung der Datensicherheit, sowie zur Unterbindung des Zugriffs durch Dritte, unternimmt TELEMED alle angemessenen und zumutbaren Schritte, welche im Rahmen der

technischen Möglichkeiten und gängigen Methoden umsetzbar sind. TELEMED kann jedoch nicht für Fehler haftbar gemacht werden, welche vom Auftraggeber oder Dritten verursacht wurden.