LEISTUNGSBESCHREIBUNG
CGM FIREWALL

GEGENSTAND DIESER LEISTUNGSBESCHREIBUNG

Die CompuGroup Medical Deutschland AG, Division Connectivity, Telematikinfrastruktur (im Folgenden CGM genannt), bietet mit der CGM Firewall ein IT-Security Produkt an, dessen Zusammensetzung und Leistungen nachfolgend beschrieben sind. Dabei können unter Ziffer 1 Allgemeine Informationen entnommen werden. Unter Ziffer 2 werden die Leistungsbestandteile beschrieben, mittels welchen das Netzwerk des Auftraggebers vor Bedrohungen aus und zu dem Internet geschützt wird. Ziffer 3 beschreibt den Umgang mit nachträglichen Anpassungen auf Wunsch des Auftraggebers und unter 4 wird der Service Level definiert.

1. ALLGEMEINE INFORMATIONEN

1.1 Hardware

Die für die Leistungserbringung gemäß dieser Leistungsbeschreibung speziell benötigte Hardware stellt CGM dem Auftraggeber zur Verfügung. Davon ausgeschlossen sind spezielle Modems für Internetanschlüsse, die vom Auftraggeber gestellt werden. Insbesondere Arbeitsplatzcomputer, Netzwerke und/oder Laptops verstehen sich nicht als spezielle Hardware gemäß dieser Leistungsbeschreibung, die von CGM bereitzustellen ist.
Datenblätter mit genauen Spezifikationen der von CGM gemäß dieser Leistungsbeschreibung zur Verfügung gestellten Hardware können jederzeit unter ***www.cgm.com/ti-download*** abgerufen werden.

1.2 Systemvoraussetzungen

Vom Auftraggeber zu stellende Voraussetzung für Installation und Nutzung der CGM Firewall 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 CGM übergeben werden.

1.3 Installationsdienstleistung

Die obligatorische Installationsdienstleistung beinhaltet die Integration der Hardware in das Netzwerk der Institution, das Einspielen der für die Institution benötigten CGM-Templates, zwei Portfreigaben und Ausnahmen im praxisüblichen Umfang, inklusive der Wiederherstellung des bestehenden WLAN-Netzwerkes bei der Installation der Firewall, sofern dies mit dem Sicherheitskonzept der Firewall vereinbar ist. Der enthaltene Remote-Service dient der Durchführung nachträglich gewünschter Änderungen und ist binnen einer Woche, nach erfolgter Inbetriebnahme vor Ort, abrufbar.

2. LEISTUNGEN DER CGM FIREWALL

Bei der CGM Firewall handelt es sich um eine Firewall-Lösung zum Schutz des gesamten Netzwerks des Auftraggebers vor Bedrohungen von außerhalb und wird daher dem lokalen Netzwerk physisch vorgeschaltet.
Die CGM Firewall Lösung besteht aus der vom Kunden käuflich erworbenen Hardware sowie der während der Vertragslaufzeit lizenzierten Firewall-Software, welche über eine cloudbasierte Managementkonsole konfiguriert wird.
Es wird ein dediziertes Gerät, die Hardware Firewall, zwischen Einwahlrouter und Praxisnetzwerk gesetzt und sämtlicher Datenverkehr (ein- und ausgehend) durch dieses geleitet. Mittels spezieller Software auf dem zwischengeschalteten Gerät werden die beschriebenen Funktionen und Regeln umgesetzt. Der erlaubte, unverschlüsselte Datenverkehr wird, bevor er ins Praxisnetzwerk gelangt, mittels verschiedener Sicherheitsfunktionen auf Bedrohungen hin untersucht. Die dazu eingesetzten und weiteren Funktionen der Hardware-Firewall sind im Folgenden beschrieben.
In der zentralen, cloudbasierten Management Konsole wird die CGM Firewall sowie das CGM Template (sprich eine durch CGM entwickelte Konfiguration der Firewall) verwaltet. CGM sowie zur Erfüllung der Leistung beauftragte DVOs können darüber Netzwerk-, Dienst- & Sicherheitskonfigurationen sowie individuelle Freischaltungen und Sperren bearbeiten. Der Zugang zu diesem System obliegt ausschließlich CGM als Betreiber sowie dem jeweiligen DVO als Erfüllungsgehilfen.
Vom Auftraggeber gewünschte Konfigurationsanpassungen (z. B. Freischaltungen) können nur auf Basis einer Beauftragung, wie im Punkt 3 *„Nachträgliche Änderungen und Ausnahmen (Exceptions)“* beschrieben, ausgeführt werden. Sämtliche Wartungsarbeiten wie Inbetriebnahme, Softwareupdates, angestoßener Neustart des Gerätes sowie Konfigurationsänderungen werden dabei in der Managementkonsole protokolliert.

2.1 Security Services

2.1.1 Content Scanning

Die über den erlaubten und unverschlüsselten Datenverkehr übertragenen Daten werden durch den “Gateway Antivirus” analysiert. Die maximale Dateigröße der zu prüfenden Daten ist auf 10 Megabyte pro Datei begrenzt.

2.2 Network Blocking

2.2.1 Botnet Detection

Ein Botnet besteht aus einer großen Anzahl von mit Malware ("Schadsoftware") infizierten Client-Computern, die von einem entfernten Server gesteuert werden, um ungewünschte Handlungen durchzuführen. Ein ferngesteuerter Command-and-Control-Server kann Botnet-Computer steuern, um diese Art von Angriffen durchzuführen:

- Denial-of-Service-Angriffe
- Versenden von Spam und Viren
- Diebstahl von gemäß der IT-Sicherheitsrichtlinien zu schützenden Daten sowie weitere auf den Endgeräten befindlichen Daten

Botnets verwenden traditionell HTTP- und IRC-Protokolle für die Kommunikation mit infizierten Botnet-Clients. Um diese Kommunikation zu blockieren, können Netzwerksicherheitsdienste den Zugriff auf diese Dienste und Ports kontrollieren.

Die CGM Firewall hat u.a. die Kategorien „Command and Control" und „Botnet Activity" aktiviert, um die Kommunikation von infizierten Botnet-Clients in Ihrem Netzwerk mit Botnet-Sites über HTTP zu blockieren. Weitere Informationen dazu finden Sie im Kapitel 2.4 Contentfilter.

Die Botnet-Kommunikation hat sich weiterentwickelt, um Sicherheitsdienste zu umgehen und andere Wege zu finden, infizierte Botnet-Clients über nicht-traditionelle Netzwerkports, soziale Netzwerke und PTP-Netzwerke zu steuern.

Der Service Botnet Detection verwendet eine Liste bekannter IP-Adressen von Botnet-Sites. Diese Botnet-Sites werden in die Liste der blockierten Sites aufgenommen, so dass die CGM Firewall diese Sites (auf Paketebene) blockieren kann. Diese Liste wird fortlaufend automatisch von CGM aktualisiert.

2.2.2. Intrusion Prevention Service (IPS)

Intrusion Prevention Service (IPS) bietet Echtzeitschutz vor Bedrohungen wie Spyware, SQL-Injektionen, Cross-Site-Scripting und Pufferüberläufen. Wenn ein neuer Angriff erkannt wird, werden die Merkmale, die den Angriff einzigartig machen, aufgezeichnet. Diese aufgezeichneten Merkmale werden als Signatur bezeichnet. IPS verwendet diese Signaturen, um Angriffe zu identifizieren.

Das von CGM zur Verfügung gestellte Template (Firewall-Konfiguration) beinhaltet den Full Scan-Modus und bietet das höchste Maß an Sicherheit.

IPS kategorisiert IPS-Signaturen in fünf Bedrohungsstufen, die auf dem Schweregrad der Bedrohung basieren. Die Schweregrade, vom höchsten zum niedrigsten, sind: „Kritisch", „Hoch", „Mittel", „Niedrig" und „Information".

Datenverkehr, der den Bedrohungsstufen „Kritisch", „Hoch", „Mittel" oder „Niedrig" entspricht, wird abgelehnt und protokolliert.

Datenverkehr, der der Bedrohungsstufe „Information" entspricht, wird standardmäßig zugelassen und nicht protokolliert.

Bei abgelehnten Anfragen wird nach der im CGM Template definierte Regelung die Verbindung getrennt und die IP-Adresse der Liste der gesperrten Sites hinzugefügt.

2.2.3 Blocked Ports

Die CGM Firewall verweigert jeglichen Datenverkehr zu blockierten Ports an allen externen Schnittstellen. Bekannte und als potenziell gefährdet eingestufte Verbindungen werden im Rahmen des Produktes gesperrt. Unter die blockierten Ports fallen: 1, 111, 513, 514, 2049, 6000, 6001, 6002, 6003, 6004, 6005, 7100 sowie 8000.

2.3. Geolocation Filter

Der Geolocation Filter versetzt die CGM Firewall in die Lage, die geografischen Standorte von Verbindungen zu und von Ihrem Netzwerk zu erkennen und Verbindungen zu oder von den angegebenen geografischen Standorten zu blockieren.

Der Geolocation Filter ist als proaktiver Schutz zu verstehen, bei dem mit dem CGM Template auf zukünftige Bedrohungen schnell und einfach reagieret werden kann.

Beispiel: Es wird ein gezielter Angriff aus einem Land auf deutsche Netze festgestellt. CGM sperrt für die Dauer dieses Angriffs die Kommunikation mit dem Herkunftsland der Bedrohung. Die Einrichtung des Auftraggebers ist somit vor dem Angriff geschützt.

2.4 Contentfilter

Der Contentfilter ist eine Lösung für Web-Sicherheit und Zugriffskontrolle, mit dem die Internetnutzung durch Mitarbeiter reguliert werden kann und gilt für alle Geräte im Netzwerk wie auch z. B. Smartphones und Tablets, welche per WLAN mit der Firewall oder einem dahinterliegenden Accesspoint verbunden sind.

Der Contentfilter kann den Aufruf von Websites gezielt steuern und dabei den Zugriff auf bestimmte Inhaltskategorien sperren.

Das CGM Template sperrt hierbei Kategorien, welche häufiger mit Sicherheitsrisiken für die IT des Auftraggebers in Verbindung gebracht werden. Folgende Kategorien werden seitens CGM 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

2.5 Firewall

Das CGM Template der Firewall wird u.a. gemäß BSI empfohlenen Sparsamkeitsprinzip betrieben und erfüllt sämtliche Voraussetzungen der IT-Sicherheitsrichtlinie in seiner aktuellen Fassung.
Dabei werden sämtliche eingehenden sowie ausgehenden Verbindungen gesperrt und nur diejenigen Verbindungen, welche wirklich benötigt werden, geöffnet.
Freigegeben im Rahmen des Produktes sind die folgenden ausgehenden Dienste:

- Softwareprodukte der CompuGroup Medical
- WEB Traffic (Ports 80, 443, 8080)
- MAIL Traffic (POP3, POP3S, SMTP, SMTPS, IMAP, IMAPS)
- DNS Nameserver
- NTP Zeitserver
- ICMP PING
- IPSec VPN (Verbindung der Telematikinfrastruktur)

3. NACHTRÄGLICHE ÄNDERUNGEN UND AUSNAHMEN (EXCEPTIONS)

Bei den verwendeten Sicherheitseinstellungen und Leistungen kann es erforderlich sein, bestimmte Dienste, Anwendungen, Ziele, Quellen, Seiten oder Ports zusätzlich freizuschalten. Ausnahmen können hinzugefügt werden, um Benutzern den Zugriff zu ermöglichen. Die Beauftragung jeglicher Konfigurationsanpassungen muss schriftlich erfolgen. Dabei obliegt es dem Auftraggeber zu prüfen, ob die Änderung im Einklang mit der IT-Sicherheitsrichtlinie nach §75b SGB V ist. Verschlüsselter HHTPS-Datenverkehr kann entschlüsselt werden, um alle verfügbaren Funktionen der Firewall auf diesen Datenstrom anwenden zu können. Dies ist ein optionaler Leistungsbestandteil, welcher nach Rücksprache mit CGM und dem zuständigen DVO angeboten werden kann.

4. SERVICE-LEVEL-AGREEMENT (SLA)

Die zugehörige SLA steht Ihnen unter **www.cgm.com/ti-download** zur Verfügung.