LEISTUNGSBESCHREIBUNG
CGM ENDPOINT 360°

GEGENSTAND DIESER LEISTUNGSBESCHREIBUNG

Die CompuGroup Medical Deutschland AG, Business Area Connectivity (im Folgenden CGM genannt), bietet mit CGM ENDPOINT 360° ein IT-Security-Produkt an, dessen Zusammensetzung und Leistung nachfolgend beschrieben wird. 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) beitragen. Ziffer 3 beschreibt den Umgang mit nachträglichen Anpassungen auf Wunsch des Auftraggebers und unter Ziffer 4 wird der Service Level definiert.

1. ALLGEMEINE INFORMATIONEN

1.1 Anzahl der PC-Arbeitsplätze

Grundsätzlich können beliebig viele Endgeräte (PC-Arbeitsplätze oder Server) mit CGM ENDPOINT 360° geschützt werden. Dabei gilt pro Endgerät (Endpoint) eine Lizenz.

1.2 Systemvorraussetzungen

Vom Auftraggeber beizustellende Voraussetzung zur Installation und Nutzung der Produkte dieser Leistungsbeschreibung ist ein breitbandiger Internetanschluss.
Die Security-Software der CGM ENDPOINT 360° wird direkt auf den Client-PC und Servern des Auftraggebers implementiert.
Es gelten die folgenden Systemvoraussetzungen:

- Windows-Workstations: Windows 8.1, Windows 10, Windows 11
- Windows-Server: 2012 R2, 2016, 2019
- MacOS-Workstations und -Server: MacOS (ab Version 10.10)

2. Leistungsbestandteile

Leistungsbestandteile, welche laut dieser Leistungsbeschreibung dem Produkt CGM ENDPOINT 360° zuzuordnen sind, schützen mit den beschriebenen Leistungen ausschließlich den Computer (Arbeitsplatz oder Server), auf dem sie installiert sind.

2.1 CGM ENDPOINT 360°

CGM ENDPOINT 360° 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. CGM ENDPOINT 360° klassifiziert alle aktiven Anwendungen in Echtzeit und stuft diese als vertrauenswürdig, schädlich oder unbekannt ein. In Verbindung mit einer Sandbox wird erkannte Schadsoftware registriert, da nach der Klassifizierung alle als unbekannt eingestuften Anwendungen im Zusammenhang in gesicherter Umgebung analysiert werden (siehe auch 2.2). Wenn die Schadsoftware bereits auf dem System des Auftraggebers vorhanden war, bevor CGM ENDPOINT 360° installiert wurde, ermöglicht die Echtzeitüberwachung die Erkennung, sobald die Schadsoftware aktiv wird, und liefert Informationen darüber, was sie seit der Installation von CGM ENDPOINT 360° getan hat. CGM ENDPOINT 360° bedient sich dabei im Folgenden genannten Methoden. Vom Auftraggeber gewünschte Konfigurationsanpassungen (z. B. Freischaltungen) können nur auf Basis einer Beauftragung, wie im Punkt 3 „Nachträgliche Änderungen" beschrieben, ausgeführt werden. Die obligatorische Installationsdienstleistung beinhaltet das Aufspielen der Software, die Einrichtung des Templates (praxisindividuelle Ausnahmen setzen) sowie einen Funktionstest.

2.1.1 Endpoint Protection Platform (EPP)

Zur Endpoint Protection Platform (EPP) gehören folgende Funktionen, welche zum aktiven Leistungsumfang beitragen:

- Ständige Multi-Vektor-Scans zur Malware-Erkennung, auch on-Demand
- Blacklisting / Whitelisting
- Vor-Ausführungs-Heuristik
- Spam- und Phishingschutz
- Manipulationsabwehr
- Mail-Inhaltsfilter

2.1.2 Endpoint Detection and Response (EDR)

Zur Endpoint Detection and Response (EDR) gehören folgende Funktionen, welche ebenfalls zum aktiven Leistungsumfang beitragen:

- Ständige Überwachung der Endpointaktivität
- Verhinderung der Ausführung unbekannter Prozesse, bis diese als vertrauenswürdig eingestuft wurden oder eine manuelle Freigabe auf Wunsch des Auftraggebers durch CGM erfolgt
- Cloudbasiertes maschinelles Erlernen von Verhaltensweisen ermöglicht die Klassifizierung sämtlicher unbekannter Prozesse (APT, Erpressungssoftware, Rootkits, etc.)
- Cloudbasiertes Sandboxing 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 CGM ENDPOINT 360° Vorkonfiguration/Einstellungen

2.2.1 Sandbox (Quarantäne in sicherer Testumgebung)

CGM ENDPOINT 360° verfügt über verschiedene Sicherheitsmodi und setzt dabei ausschließlich auf den unten beschriebenen Hardening Modus. Dabei werden potenzielle Bedrohungen 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 zu 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. CGM ENDPOINT 360° 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.

Betriebsmodus: Hardening
Schädliche Programme werden entfernt. Unbekannte und somit potenziell schädliche Programme, die aus dem Internet, von anderen Netzwerkcomputern oder von externen Laufwerken stammen, werden blockiert, bis mittels der cloudbasierten Analyse bestimmt wurde, ob es sich um Schadsoftware handelt oder nicht. Andere unbekannte Programme, z. B. solche, die sich bereits vor der Installation von CGM ENDPOINT 360° auf dem PC befunden haben, werden zunächst zur Ausführung zugelassen, während sie analysiert werden.

2.2.2 Anti-Exploit

Der aktive Anti-Exploit-Schutz hindert schädliche Programme daran, bekannte und unbekannte (Zero-Day-Attacken) Schwachstellen in Anwendungen auszunutzen, um auf Endgeräte im Auftraggebernetzwerk zuzugreifen.

2.2.3 Virenschutz

CGM ENDPOINT 360° enthält einen klassischen Virenschutz (EPP – Endpoint Protection Platform) mit folgenden aktivierten Funktionen:

- Datei-Virenschutz
- E-Mail-Virenschutz
- Webbrowsing-Virenschutz sowie folgende zu erkennende Bedrohungen:
  - Viren erkennen
  - Hacker-Tools und potenziell unerwünschte Programme (PUP) erkennen
  - Schädliche Aktionen blockieren
  - Phishing erkennen

2.2.4 Contentfilter

Der Contentfilter ist eine Lösung für Web-Sicherheit und Zugriffskontrolle, mit dem die Internetnutzung durch Mitarbeiter reguliert werden kann.

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.

- Adult Material – Adult Content
- Adult Materia – Sex
- Extended Protection – Dynamic DNS
- Extended Protection – Elevated Exposure
- Extended Protection – Emerging Exploits
- Extended Protection – Suspicious Content
- Information Technology – Hacking
- Information Technology – Proxy Avoidance

2.2.5 Autorisierte Software

Im CGM ENDPOINT 360° Template sind alle digitalen Signaturen für Softwareprodukte der CompuGroup Medical eingespielt. Dadurch werden autorisierte Programme während der Klassifizierung nicht blockiert. Der Zero-Trust Application Service klassifiziert und blockiert oder desinfiziert sie jedoch, wenn sie sich als Malware oder PUPs herausstellen.

2.2.6 Threat Hunting Service (Angriffsindikatoren)

Der aktive Threat Hunting and Investigation Service wird betrieben, um Hacking- und Living-off-the-Land-Techniken zu erkennen. Durch die Schlussfolgerungen verbessern sich die Algorithmen für maschinelles Lernen. Analysiert wird jeder verdächtige Fall auf Angriffsindikatoren, welche dann untersucht werden, um im Ereignisstrom Evasions- und Kompromittierungstechniken (TTPs) ausfindig zu machen. Der Service sucht außerdem proaktiv nach Mustern für ungewöhnliche Verhaltensweisen, die nicht zuvor durch das Netzwerk identifiziert wurden.

2.3 CGM ENDPOINT 360° AddOns / Zusatzmodule

2.3.1 Patch Management

Patch Management ist ein Modul zum Schwachstellenmanagement von Betriebssystemen und Drittanbieter-Anwendungen auf Windows-Workstations und -Servern, welches eine zentralisierte Echtzeit-Sicherheitsstatusübersicht für alle Software-Schwachstellen, fehlende Patches, Updates und nicht mehr unterstützte End of Life (EOL) – Software bietet sowie benutzerfreundliche Tools für den gesamten Patch-Management-Zyklus: Von der Ermittlung bis hin zur Installation und Überwachung der Endpoints. CGM installiert mit Patch Management automatisch ausschließlich sicherheitsrelevante Updates (Microsoft und Drittanbieter). Eine aktuelle sowie vollständige Übersicht der Software, welche von Patch Management mit Sicherheitsupdates versorgt wird, wird vom Hersteller unter https://info.pandasecurity.com/patchmanagementapp/ bereitgestellt. Dabei werden alle sicherheitsrelevanten Patches zyklisch installiert. Ein Zyklus entspricht sieben Kalendertagen. Ausschlüsse von Software-Patches (z. B. Java) bei bekannten Problemen (z. B. BlueScreen) mit dem Betriebssystem können optional mit dem Endkunden abgesprochen werden. Patch Management ist vollständig in CGM ENDPOINT 360° integriert und setzt damit keinerlei neue Endpoint-Agenten oder Verwaltungskonsolen voraus. Die Updates (Microsoft und Drittanbieter) werden von CGM nicht auf Funktionalität / Kompatibilität überprüft.

3. Nachträgliche Änderungen

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 ist.

4. SERVICE-LEVEL-AGREEMENT (SLA) Servicezeiten / Servicebereitschaft

Für CGM PROTECT Bestandskunden mit Vertragsbeginn vor 15.06.2023 gelten die CGM PROTECT SLA, welche unter **cgm.com**/ti-download einzusehen und herunterzuladen sind.

Für CGM PROTECT Neukunden mit Vertragsbeginn ab 15.06.2023 gelten die CGM CONNECTIVTY SLA, welche ebenfalls unter **cgm.com**/ti-download einzusehen und herunterzuladen sind.

CompuGroup Medical Deutschland AG
Business Area Connectivity
Maria Trost 21 | 56070 Koblenz

cgm.com/de

CGMCOM-27544_CONPRO_0824_LBR

Synchronizing Healthcare

CompuGroup Medical