LEISTUNGSBESCHREIBUNG

CGM PROTECT ENDPOINT 360°

GEGENSTAND DIESER LEISTUNGSBESCHREIBUNG

Die CompuGroup Medical Deutschland AG, Division Connectivity, Telematikinfrastruktur (im Folgenden CGM genannt), bietet mit CGM PROTECT 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 PROTECT 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 PROTECT 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-Server:** 2012 R2, 2016, 2019
· **MacOS-Workstations und -Server:** MacOS (ab Version 10.10)

2. LEISTUNGSBESTANDTEILE

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

2.1. CGM PROTECT Endpoint 360°

CGM PROTECT 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 PROTECT 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 PROTECT 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 PROTECT Endpoint 360° getan hat. CGM PROTECT 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 & Ausnahmen (Exceptions) beschrieben, ausgeführt werden.

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

CGMCOM-7026_c1187_LB_Endpoint_0822_KS

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 PROTECT Endpoint 360° Vorkonfiguration/Einstellungen

2.2.1. Sandbox (Quarantäne in sicherer Testumgebung)

CGM PROTECT 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 PROTECT 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 Analysebestimmt wurde, ob es sich um Schadsoftware handelt oder nicht. Andere unbekannte Programme, z. B. solche die sich bereits vor der Installation von CGM PROTECT 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 Auftragggebernetzwerk zuzugreifen.

2.2.3. Viren Schutz

CGM PROTECT 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 PUPs 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 Material - 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

In dem CGM PROTECT 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.

3. NACHTRÄGLICHE ÄNDERUNGEN

Bei den verwendeten Sicherheits-Einstellungen & 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.

4. SERVICE-LEVEL-AGREEMENT (SLA)

4.1 Servicezeiten / Servicebereitschaft

Service- und Supportanliegen meldet der Auftraggeber unter Nennung aller erforderlichen Daten, insbesondere seiner Kundennummer grundsätzlich per Telefon, Fax oder E-Mail und sofern vorhanden über die dafür vorgesehenen Formulare, welche unter www.cgm.com/ti-download zur Verfügung stehen. Die Annahme und Bearbeitung von Service- und Supportanliegen erfolgt werktags – ausgenommen samstags – in der Zeit zwischen 08:00 Uhr und 18:00 Uhr.

4.2 Reaktionszeiten

CGM reagiert binnen vier Stunden innerhalb der Servicezeiten ab Meldung des Service- oder Supportanliegens. Als Meldung gilt hierbei die telefonische Übermittlung des Anliegens über die dem Auftraggeber mitgeteilte Servicerufnummer 0261 8000 2097.
Meldungen, die nachts in der Zeit zwischen 18:00 Uhr und 08:00 Uhr, samstags, sonntags oder an bundeseinheitlichen Feiertagen eingehen, beginnt die Reaktionszeit am folgenden Werktag um 08:00 Uhr. .

4.3 Bearbeitungszeit

CGM bearbeitet die Service- und Supportanliegen remote innerhalb von 48 Stunden während der angegebenen Servicebereitschaftszeiten. Die Bearbeitungszeit beginnt, mit Ablauf der Reaktionszeit, jedoch frühestens sobald alle erforderlichen Angaben durch den Auftraggeber gemacht wurden.