redIT

MANAGED ENDPOINT SECURITY ESSENTIALS

LEISTUNGSBESCHREIBUNG / NUTZUNGSBEDINGUNG

Inhaltsverzeichnis

1 EINLEITUNG

Managed Endpoint Security Essentials sorgt dafür, dass alle Windows Clients kontinuierlich überwacht, aktualisiert und geschützt werden. Sie beinhaltet Funktionen wie Antivirus-Software, Firewalls und regelmässige Sicherheitsupdates von Windows und Drittherstellerapplikationen, um Bedrohungen abzuwehren und die Integrität der Daten zu gewährleisten.

Managed Endpoint Security Essentials richtet sich besonders an Schweizer KMU, die ihre IT-Sicherheit auf ein professionelles Niveau heben möchten, ohne dabei zwingend interne Ressourcen zu belasten. Diese Dienstleistung ist ideal für Organisationen, die keine hausinternen IT-Sicherheitsexperten haben oder deren Teams bereits ausgelastet sind und Unterstützung bei der Endpunktsicherheit benötigen. Auch Unternehmen, die auf eine hohe Verfügbarkeit und Zuverlässigkeit ihrer IT-Infrastruktur angewiesen sind, profitieren von den umfassenden Schutzmassnahmen und der kontinuierlichen Überwachung durch erfahrene Sicherheitsspezialisten.

2 PRODUKTSPEZIFIKATIONEN

2.1 Initiale Einrichtung

Die initiale Einrichtung bringt die Grundlage, damit die Geräte im Unternehmen korrekt durch redIT verwaltet werden können.

2.2 Konformitäts- und Sicherheitsrichtlinien

Unter anderem werden folgende Konformitäts- und Sicherheitsrichtlinien gesetzt und überwacht:

- Windows Firewall
- Antivirus und Antispyware
- Harddisk Verschlüsselung (Bitlocker)
- Secure Boot (Windows 11)
- Windows und Microsoft 365 Apps Updates
- Cloud Sicherung der Windows Ereignisprotokolle
- Credential Guard
- Serviceende der Windows Version (Build nicht End of Life)

2.3 Dritthersteller Updates

Aktualisierung der gängigsten Dritthersteller Anwendungen (> 800’000), welche in den folgenden vertrauenswürdigen Quellen verfügbar sind:

- Microsoft Store
- Winget Repository

Die fortlaufende Verfügbarkeit von Softwareupdates kann nicht garantiert werden. redIT übernimmt keine Haftung für die in den Quellen enthaltenen Softwareupdates und deren Funktionalität.

2.4 Software Schwachstellen Management

Prüfen der installierten Software (Betriebssystems und installierte Applikationen) auf bekannte kritische Sicherheitslücken. Direktes Umsetzen oder vorschlagen von Massnahmen, um diese Sicherheitslücken zu schliessen.

2.5 Monatlicher Bericht

Sie erhalten monatlich einen Sicherheitsbericht der Windows Endgeräte.

Dieser Bericht enthält Abweichungen zu:

- den definierten Konformitäts- und Sicherheitsrichtlinien
- aktiven kritische Software-Schwachstellen und unsere Empfehlungen dazu
- geleistete und geplante Interventionen zur Sicherstellung der Konformität und Sicherheit der Endgeräte

3 VORAUSSETZUNGEN

Für den Einsatz des redIT Managed Endpoint gelten untenstehende Voraussetzungen. Es müssen nicht alle Voraussetzungen erfüllt sein, jedoch können entsprechenden Teile dann nicht überwacht werden. Bitte sprechen sie uns in diesem Falle vorher an.

Voraussetzungen:

- Microsoft Windows Clients mit Pro/Business/Enterprise Betriebssystem, welches sich noch im Mainstream Support befindet.
- x64 Prozessorarchitektur (Intel/AMD)
- Zugang zum Microsoft Windows Store
- Geräte sind in der Entra ID vorhanden
- Geräte sind Intune verwaltet inklusive primärer Benutzer und Geräteeigentümer
- Als Antivirus Dienst wird Microsoft Defender eingesetzt
- Alle Benutzer/Geräte verfügen über eine der folgenden Lizenzen:
    - Microsoft Business Premium
    - Microsoft 365 E5
    - weitere Lizenzkombinationen sind auf Anfrage verfügbar
- Die Endpunkte verfügen über Internetkonnektivität
- redIT benötigt auf dem zu verwalteten Microsoft 365 Tenant über GDAP (granular delegated administrative privilege) entsprechende Rollen, um den Betrieb des Produktes zu gewährleisten.
- Der Service muss für sämtliche in Intune/Entra ID eingebundenen Windows Clients bezogen werden
- Die Endgeräte müssen monatlich mehrmals mit dem Internet verbunden sein
- Endgeräte müssen wöchentlich neu gestartet werden
- Die Durchführung von Windows Updates darf maximal 24h verschoben/pausiert werden
- Nicht mehr verwendete Geräte müssen aus Intune/Entra ID entfernt werden

4 NICHT ENTHALTENE LEISTUNGEN

- Benötigte Microsoft Lizenzen
- Softwareupdates von Dritthersteller Applikationen welche nicht den Quellen gemäss Kapitel «Dritthersteller Updates» verfügbar sind
- Die in diesem Angebot enthaltenen Interventionen sind begrenzt auf einen Guthabenpool (10 Minuten pro Endgerät). Darüberhinausgehende Interventionen erfolgen kostenpflichtig nach Absprache mit dem Kunden

5 ALLGEMEINE BESTIMMUNGEN

- Die Kündigungsfrist beträgt 20 Tage
- Die Implementierungszeit beträgt 2-4 Wochen
- Kundenseitige Mengenanpassungen müssen redIT Services AG innerhalb von 30 Tagen gemeldet werden
- Produktanpassungen innerhalb der Vertragslaufzeit sind vorbehalten
- redIT Services AG behält sich vor, Aufträge abzulehnen
- Haftungsausschluss: redIT Services AG haftet nicht für Folgeschäden, die durch die Nutzung unserer Produkte oder Dienstleistungen entstehen. Weiterhin wird jegliche Gewährleistung für die Funktionalität der Dienste ausgeschlossen. Der Kunde akzeptiert, dass die Nutzung der Dienste auf eigenes Risiko erfolgt.
- Es gelten unsere Allgemeinen Geschäftsbestimmungen