Datensicherheit MSP Remote Monitoring & Management

Wer hat direkten Zugriff auf kundenspezifische Daten?
Nur Mitarbeiter des Unternehmens Solarwinds MSP haben Zugriff direkt auf die Server. Es werden zur Verbindung verschlüsselte Benutzernamen und Passwörter verwendet, sowie nur ein bestimmter IP-Kreis für Verbindung zugelassen. Die einzige Information, die bislang über Kunden abgelegt werden, ist deren Name oder Kundennummer, ggfls. Kontaktdetails, allgemeine Serverinformationen (wie der Name des Servers unter dem dieser im Dashboard aufgeführt wird etc.) der Dashboard Login, sowie die Checks, welche pro Gerät ausgeführt werden. Jegliche zusätzlichen Informationen wie bspw. Proxy Server Logins etc. werden NUR lokal auf dem Gerät gespeichert und niemals an Solarwinds MSP übertragen.
Da keinerlei Logins zu den Server Systemen gespeichert werden, wäre es nicht möglich, sich mit den vom MSP Remote Monitoring & Management gesammelten Daten Zugriff zu Kundensystem zu verschaffen.

Gibt es Protokolle über den Verbindungsaufbau zu den Servern?
Wie oben beschrieben werden die Verbindungen zu den Hauptservern aus einem spezifischen IP-Kreis über HTTPS aufgebaut, welcher nur Mitarbeitern der Entwicklungsabteilung von Solarwinds MSP gestattet ist.

Wie lange werden die gesammelten Daten gespeichert?
Die einzigen Daten, die durch den „Advanced Monitoring Agent“ gesammelt werden, sind einige grundlegende Informationen (Betriebssystem etc.), einige Daten zu den ausgeführten Prüfungen (z.B. a 1 oder 0 für Check erfolgreich oder fehlerhaft, verfügbarer Festplattenplatz, Antivirus Pattern Version etc.) mitsamt einem einzigartigen Schlüssel, welcher dem Server zur Identifikation vom MSP Remote Monitoring & Management zugewiesen wird.
Dies zusammen wird genutzt um die Serverdetails im Dashboard anzeigen zu können.
Es werden Check-Fehlschlag-Informationen für Berichte (täglicher, wöchentlicher, monatlicher Bericht und Fehlerverlauf) vorgehalten, jedoch werden die Daten mit jedem Mal, wenn ein Bericht generiert wird, wieder zurückgesetzt.
Alle im System hinterlegten Informationen bzgl. eines Servers werden beim Deinstallieren des Server Agenten aus der Datenbank entfernt (mehr dazu weiter unten).

Gibt es Informationen zu den Maßnahmen der Datensicherung mit denen der MSP Remote Monitoring & Management Datenbankserver gesichert wird?
Jede Nacht wird ein Full-Backup der Datenbank erstellt. Ebenfalls werden die Backupmedien außerhalb des Rechenzentrums abgelegt um die Sicherheit zu maximieren.

Was passiert mit Kundendaten wenn dieser den MSP Remote Monitoring & Management-Dienst kündigt? Gibt es Protokolle über die Datenvernichtung?
Wie bereits oben erwähnt werden Server, die nicht mehr überwacht werden, ebenfalls aus der Datenbank gelöscht. Es wird lediglich der Name der Kunde/Standort/Servername behalten für den Fall, dass der Server neuinstalliert wird um eine weitere Aktivierungsgebühr zu verhindern. Die übliche Herangehensweise zum Entfernen der Serverüberwachung ist die herkömmliche Deinstallation über Systemsteuerung -> Software -> Deinstallieren. Falls das nicht klappen sollte, ist es möglich, den Server direkt im Dashboard zu löschen. Seit der dem Dashboard-Release v5.45.1 zieht dies eine automatische Deinstallationsroutine des Agenten am lokalen System nach sich.

Auf welche Art und Weise kommuniziert der Agent mit dem zentralen Host Server?
Alle Agentenkommunikationen zu diesem Server sind via SSL verschlüsselt. Proxy-Server (SOCKS5 und HTTP) sind unterstützt. Der Agent benutzt NTLM bzw. grundlegende Authentifizierungen. Er nutzt mehrere Server zum Upload, so dass er beim Ausfall eines Server einen anderen Weg wählen kann.

Welche Daten werden erfasst?
Die einzigen Daten, die MSP Remote Monitoring & Management erfasst, sind grundlegende Konfigurationsinformationen Ihrer Server, Betriebssysteme etc., einige Daten, die mit den Checks zusammenhängen (z.B. Laufwerksgröße, Anti-Virus-Version, 1 oder 0 Checks für Erfolg oder Fehlschlag) und

einzigartige Identifikationsnummern, die dem Server zugewiesen sind. Diese Informationen werden gesammelt, um Sie auf der Übersichtskonsole anzuzeigen.

Welche Sicherheit wird verwendet um andere Firmen/Institutionen/Individuen davon abzuhalten, auf vertrauliche Daten zuzugreifen?
Die **einzigen** Informationen, die MSP Remote Monitoring & Management über die Kunden ablegt, sind deren Name und Kontaktdetails (sofern eingegeben) und Server-Informationen wie bspw. der Servername, die MSP Remote Monitoring & Management-Zugangsdaten zur Verwaltung der Benutzer und die Checks, die für einzelne Geräte eingestellt wurden. Zusätzliche Informationen wie die Proxy-Server-Logins oder lokale Autorisierungen werden lokal auf dem jeweiligen Client gespeichert und niemals an Solarwinds MSP weitergeleitet. Da Solarwinds MSP keine Informationen über Server-Logins speichert, ist es unmöglich, mit den gesammelten Daten Zugang zu Ihren Systemen zu erlangen.

Wie viel der vom MSP Remote Monitoring & Management gesammelten Daten werden mit dem lokal installierten Agenten gespeichert?
Das MSP Remote Monitoring & Management bewahrt auf den Kundenservern die Konfigurations-Check-XML-Datei, die Check-Logdatei, die Upload-Logdatei, eine Liste von Diensten, die auf der Maschine gefunden wurden, in der service.ini au. Die MSP Remote Monitoring & Management-Agenten-Konfiguration wird in der settings.ini abgespeichert. In den Agenten eingegebene Passwörter werden verschlüsselt und nur auf der lokalen Maschine gesichert.

Wo befinden sich die zentralen MSP Remote Monitoring & Management Server? Wie sicher sind diese?
Die Server befinden sich in Köln, Deutschland und werden bei HostEurope bereitgestellt.
Weitere Informationen entnehmen Sie bitte dem Dokument „MAX RM - Überblick über das deutsche Rechenzentrum.pdf“

Beispiel der übertragenen Daten:

24x7:
16872,1004,5,0,3,"C:\","13","3","68315|18085"
16872,1013,5,0,3,"Backup Exec Remote Agent for Windows Servers","1","0",""
16872,1013,5,0,3,"Backup Exec Agent Browser","1","0",""
16872,1013,5,0,3,"Backup Exec Device & Media Service","1","0",""
16872,1013,5,0,3,"Backup Exec Job Engine","1","0",""
16872,1013,5,0,3,"Backup Exec Server","1","0",""
16872,1013,5,0,3,"DNS Client","1","0",""
16872,1013,5,0,3,"Event Log","1","0",""
16872,1013,5,0,3,"Server","1","0",""
16872,1013,5,0,3,"SQL Server (BKUPEXEC)","1","0",""
16872,1013,5,0,3,"Terminal Services","1","0",""
16872,1013,5,0,3,"Automatic Updates","1","0",""
16872,1013,5,0,3,"Wireless Configuration","1","0",""

TSC:
16872,1001,5,0,2,"McAfee Viruscan","MTWTFSS","5272"
16872,1003,5,0,2,"C:\","25","68315|18085|0"