Verlässliche VPN-Lösungen in Industrie 4.0/M2M-Umgebungen

Im Internet der Dinge werden immer mehr Gegenstände des alltäglichen Lebens miteinander vernetzt. Daher stehen Unternehmen und Sicherheitsexperten vor der Herausforderung, die Kommunikation von Millionen von Geräten zu schützen. Geldautomaten, Verkaufsautomaten, Fahrzeuge, Lagertechnikgeräte, Ortungsgeräte für Transporte und Anlagen — die Liste der IoT-Anwendungen und M2M (Machine-to-Machine)-Umgebungen wird immer länger.

Wie verwaltet man ein sicheres VPN ohne menschliche Interaktion an der Schnittstelle zum Endgerät? Ist keine verlässliche Lösung vorhanden — dies gilt insbesondere bei geschäftskritischen Systemen — besteht das Risiko von Gewinneinbußen, unzufriedenen Kunden oder Nutzern und von zusätzlich erforderlichem Aufwand für die Wiederherstellung des Betriebs. Bei Systemen, in denen es um sensible Daten geht, kann zudem die Einhaltung von Sicherheitsanforderungen gemäß PCI, SOX oder HIPPAA besonders wichtig sein.

Wie viele M2M-Verbindungen?

*Die Prognosen der Analysten variieren stark, die Wachstumsrate ist jedoch unbestritten. Vorhersagen reichen von 12 Milliarden bis zu 50 Milliarden verbundener Geräte bis zum Jahr 2020. Die jährliche Zuwachsrate beträgt knapp 23.**

Für die Anbindung einer Maschine an ein Netzwerk gibt es verschiedene Möglichkeiten. Meist sind zusätzliche Hardwarekomponenten und Dienstleistungen nötig, um einen privaten kabellosen Anschluss bereitzustellen oder ein Gerät zur Verbindung der Maschine mit dem Netzwerk zu verwenden. Der einfachste und sicherste Weg, eine Maschine über ein VPN mit einem Netzwerk zu verbinden, ist die Nutzung eines VPN-Clients auf dem Gerät. Diese Lösung lässt sich leicht in die vorhandene Infrastruktur einbinden und erfordert keine zusätzliche Hardware, wie beispielsweise Router, Modems oder SIM-Karten. Darüber hinaus erfolgt die Sicherung des Datenverkehrs direkt über die laufende Maschine anstatt über den kabellosen Anschluss oder Router. Unverschlüsselte Daten verlassen somit niemals das Gerät.

Unterschiedliche Umgebungen erfordern selbstverständlich unterschiedliche Maßnahmen. In diesem Whitepaper werden drei Bereiche vorgestellt, die beim Einrichten eines VPNs in einer INDUSTRIE 4.0/M2M-Umgebung berücksichtigt werden sollten.

Verbindungen — Wie wird eine ordnungsgemäße Anbindung der Maschine sichergestellt?
Authentifizierung — Wie wird eine sichere Authentifizierung der Maschine gewährleistet?
Management — Wie wird das VPN den Sicherheitsrichtlinien des Unternehmens entsprechend?

*Quelle:http://www.mordorintelligence.com/industry-reports/machine-to-machine-m2m-services-market

Aufbau der Verbindung

Abhängig von der Maschinen-Anwendung ist möglicherweise eine ständige VPN-Verbindung erforderlich (wie etwa bei einer Überwachungskamera) oder nur im Bedarfsfall (bsp. beim Bezahlen mit einer Kreditkarte am POS-Terminal). In jedem Fall muss der VPN-Client eine zuverlässige VPN-Session aufbauen können. Im Vordergrund steht die Wahl einer den Anforderungen entsprechenden Verbindungsmethode.

Automatisch oder „Always On“

Eine Vorgehensweise besteht darin, dass der VPN-Client sich automatisch mit dem VPN verbindet und diese Verbindung bestehen bleibt. Sollte die Verbindung unterbrochen werden — beispielsweise aufgrund von Netzwerkproblemen — wird der VPN-Client versuchen, die Sitzung wieder herzustellen. Dies garantiert, dass das VPN wieder aktiviert ist, sobald eine Datenverbindung verfügbar ist. Beim Seamless Roaming errichtet der VPN-Client die Verbindung automatisch und behält die Session im Falle einer Unterbrechung bei. So wird ein Session-Verlust der laufenden Anwendung an der Maschine verhindert bis die VPN-Verbindung wieder hergestellt werden kann.

Kommandozeile

Soll das VPN vorzugsweise direkt gesteuert und eine VPN-Session nur bei Bedarf aufgebaut werden, kann ein Kommandozeilen-Tool zur Interaktion zwischen der Anwender-Software der Maschine und dem VPN-Client verwendet werden. Normalerweise unterstützt ein Kommandozeilen-Tool Grundfunktionen, wie etwa verbinden/trennen, Eingabe von Nutzername/Passwort und Start/Stopp des VPN-Clients.

API

Ein sehr wirkungsvoller Ansatz ist die Verwendung eines API (Application Programming Interface). Dies ermöglicht die komplette Steuerung des VPN-Clients über die Anwender-Software des Geräts. Ein API besitzt zusätzlich zu den Funktionalitäten eines Kommandozeilen-Tools weitere Funktionalitäten: Beispielsweise lässt sich mit Hilfe eines API das VPN-Profil verändern, um so die Verbindung zu einem anderen Gateway zu ermöglichen. Es kann auch eingesetzt werden, um eine PIN zur Verwendung von Zertifikaten einzugeben, den Software-/Verbindungs-/Authentisierungs-Status abzufragen oder bestimmte Einstellungen zu verändern.

Authentifizierung der Verbindung

In den meisten INDUSTRIE 4.0/M2M-Umgebungen gibt es kein Personal für die Eingabe von Zugangsdaten oder PINs. Damit dennoch dasselbe Sicherheitsniveau erreicht wird, muss die Maschine oder der VPN-„Nutzer“ den Authentifizierungsvorgang beim Aufbau einer VPN-Verbindung selbst durchführen können. Abhängig von den Sicherheitsanforderungen der Anwendung und den Richtlinien im Unternehmen sind mehrere Methoden möglich.

Nutzername/Passwort

In der VPN-Client-Konfiguration auf dem Gerät lässt sich ein Nutzername/Passwort speichern. Nutzername/Passwort kann eine Information über das Gerät sein, beispielsweise der Hostname. Möglicherweise wird das Gerät auch von verschiedenen Menschen mit eigenständigen Nutzername/Passwort-Kombinationen verwendet, so wie etwa ein Firmenwagen von mehreren Personen genutzt wird.

Zertifikate (PKI – Public Key Infrastructure)

Durch Nutzung der asymmetrischen Verschlüsselung lässt sich eine noch stärkere Authentisierung erreichen. Dazu können Zertifikate nach Wahl implementiert werden. Die Kombination von Zertifikaten mit Nutzername/Passwort-Authorisierung oder sogar Zwei-Faktor-Authentifizierung sorgen ebenfalls für ein höheres Sicherheitsniveau. Einige Zertifikate sind softwarebasiert, während andere in Verbindung mit der Maschine, einer Smartcard oder einem in die Maschine eingebauten Chip funktionieren:

- **Soft-Zertifikate** oder Benutzer-Zertifikate sind Dateien, welche sich von einem Gerät auf ein anderes kopieren lassen. Das bedeutet, sie sind nicht an ein bestimmtes Gerät gebunden. Je nach Anforderungen kann dies ein Vorteil oder ein Nachteil sein. Es kann eine herkömmliche .p12-Datei verwendet werden oder auch die im Betriebssystem (bsp. im Zertifikatsspeicher von Microsoft) gespeicherten Soft-Zertifikate. Je nach VPN-Konfiguration erfordert das Zertifikat eventuell eine PIN.

- **Maschinen-/Hardware-Zertifikate** sind Benutzer-/Soft-Zertifikate, die mittels „Fingerprint“ der Maschine an genau diese eine Maschine gebunden sind und somit mit keiner anderen verwendet werden können.

- **Smartcards** sind Karten (wie etwa Kreditkarten) mit eingebetteten, integrierten Chips. Ein Soft-Zertifikat wird auf dem Chip gespeichert und lässt sich somit nicht exportieren. Smartcards bieten eine zusätzliche Sicherheitsschicht, da zur Authentifizierung die externe Karte physisch

vorliegen muss. Diese Methode erfordert einen Smartcard-Reader, der in die Maschine eingebaut oder an diese angeschlossen wird.

- **TPM (Trusted Platform Module)** ist eine in die Maschine eingebaute Smartcard. Dieser preiswerte Crypto-Chip verfügt über eine geringe Leistungsfähigkeit sowie eine geringe Kapazität und wird auf das Motherboard gelötet. Dies macht die Implementierung des Verfahrens im Vergleich zur Implementierung anderer Authentifizierungsverfahren komplizierter. Der Chip verfügt über die gleichen Funktionen wie der einer Smartcard, bietet jedoch zusätzlich Root-of-Trust-Security. Ein TPM-Zertifikat kann mit oder ohne PIN verwendet werden.

Authentifizierungsverfahren auf einen Blick

Authentifizierungs-verfahren	Ressourcen/ Zeit	Flexibilität	Sicherheit	Ver-schlüsselung	Kommentare
Nutzername/ Passwort	Niedrig	Hoch	*	Symmetrisch	Eine Anwenderverzeichnis-Infrastruktur (zum Beispiel LDAP, Active Directory, RADIUS) muss bereits vorhanden sein.
Soft-Zertifikate	Niedrig	Mittel	***	Asymmetrisch	Gewöhnlich ist bereits eine CA (Certification Authority, Zertifizierungsstelle), beispielsweise Microsoft CA oder Entrust, vorhanden.
Hardware-/ Maschinen-Zertifikate	Niedrig	Niedrig/ Mittel	****	Asymmetrisch	Die Verschlüsselung funktioniert in Verbindung mit der Maschinen-Hardware.
Smartcards	Hoch	Niedrig	*****	Asymmetrisch	Auf (externen) Smartcards werden Soft-Zertifikate verwendet. Zusätzliche Hardware und externe Dienstleister sind erforderlich.
TPM	Hoch	Niedrig	*****	Asymmetrisch	Das Zertifikat ist auf einem verschlüsselten Chip in der Maschine gespeichert. Ein externer Dienstleister ist erforderlich.

Management des VPN-Clients

Über ein VPN kann jede Maschine sicher mit dem Netzwerk verbunden werden. Ohne funktionierendes VPN kann die Maschine ihren Zweck nicht erfüllen. Daher muss sichergestellt sein, dass ein VPN-Management-Tool vorhanden ist — sei es für Updates der Konfiguration, für Software-Updates oder für die Verwaltung der Zertifikate. Ohne zentrales Management muss der Rollout von Konfigurationen manuell über einen Speicher-Stick oder eine CD erfolgen. Dazu muss jedes Mal, wenn eine Änderung notwendig ist, ein direkter Zugriff an jeder einzelnen Maschine stattfinden.

Rollout

Bei der Verwendung eines System-Abbilds oder eines Softwareverteilungssystems wird der VPN-Client mit einer Erstkonfiguration für den Verbindungsaufbau geliefert. Sobald der VPN-Client Kontakt zum Management-Server erhält, ist ein automatischer Download von individuellen Konfigurationen, Zertifikaten (falls erforderlich), Lizenzen und Software-Updates (falls erforderlich) möglich.

Konfigurations- und Software-Updates

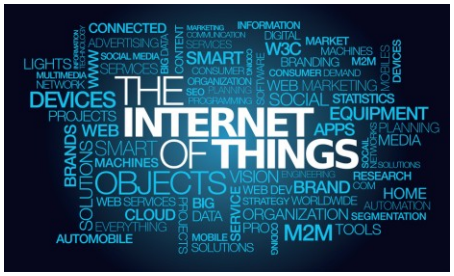
Der VPN-Client verbindet sich regelmäßig mit dem Managementsystem und überprüft, ob neue Konfigurationen oder Softwareversionen verfügbar sind. Ist dies der Fall, erfolgt automatisch die Installation auf dem Client. Dazu ist keine physische Interaktion mit der Maschine erforderlich.

VPN-Management

Ein zentrales Management gewährleistet, dass trotz der Expansion der INDUSTRIE 4.0/M2M-Umgebung und der steigenden Anzahl der Endgeräte das Netzwerk niemals zu komplex für einen sicheren und effizienten Betrieb wird. Ein Single Point of Administration bietet Flexibilität bei der automatischen Skalierung entsprechend der geschäftlichen Anforderungen.

Authentifizierungsmanagement

Bei der Verwendung von Zertifikaten zur Authentifizierung kann ein PKI-Management-Tool Unterstützung bei Rollout, Ausgabe, Sperrung oder Erneuerung von Zertifikaten bieten. Auch dazu müssen die Endgeräte nicht berührt werden.



Zusammenfassung

Falls keine stabilen VPN-Verbindungen in der INDUSTRIE 4.0/M2M-Umgebung zur Verfügung stehen, besteht für die Maschinen das Risiko von Störungen oder Ausfällen. Das verursacht zusätzlichen Aufwand und oft auch Gewinneinbußen. Sind Maschinen über große geographische Entfernungen verteilt, kann ein physischer Zugriff schwierig, zeitaufwendig und teuer sein. In jedem Fall ist es eine größere Aufgabe. Die gesamte Kommunikation zwischen der Maschine und dem Unternehmensnetzwerk basiert auf einer stabilen VPN-Verbindung. Sorgen Sie für automatisch skalierbare VPN-Software – wie beispielsweise Software von NCP –, um Tausende von Maschinen im Netzwerk und deren Interaktion mit dem Rechenzentrum zu verwalten.

Über Julian Weinberger

Julian Weinberger, CISSP, ist Director of Systems Engineering bei NCP engineering. Er verfügt über eine zehnjährige Erfahrung in der Netzwerk- und Sicherheitsindustrie sowie umfangreiches Fachwissen in den Bereichen SSL-VPN, IPsec, PKI und Firewalls. Julian Weinberger lebt in Mountain View, Kalifornien und ist verantwortlich für die Entwicklung von IT-Netzwerksicherheitslösungen und Unternehmensstrategien von NCP engineering. Außerdem bietet er Großkunden des Unternehmens technischen Support für ihre Remote Access-Sicherheitslösungen, sowohl vor als auch nach dem Kauf.

About NCP engineering

Seit der Firmengründung 1986 liefert NCP engineering innovative Software. Diese ermöglicht Unternehmen, ihren Remote Access neu zu überdenken und Schwierigkeiten im Zusammenhang mit Aufbau, Verwaltung und Instandhaltung eines sicheren Netzwerkzugangs für Mitarbeiter zu beseitigen.

Mit Firmensitzen in Nürnberg, Deutschland und in der San Francisco Bay Area in Nordamerika hat das Unternehmen weltweit über 35.000 Kunden. Dazu zählen Unternehmen aus den Bereichen Gesundheitswesen, Finanzen, Bildung und Regierung sowie viele Fortune-500-Unternehmen. Zur Betreuung der Kunden hat NCP zusätzlich ein Netzwerk aus nationalen sowie regionalen Technologie-, Channel- und OEM-Partnern errichtet.

Wenn Sie mehr über NCPs Remote Access VPN-Lösungen erfahren möchten, dann besuchen Sie www.ncp-e.com. Kontaktieren Sie uns auch über unseren Blog, VPN Haus oder über Twitter @NCP_engineering.

Haftungsausschluss

Die in diesem Dokument enthaltenen Informationen können ohne Vorankündigung geändert werden und stellen keine Verpflichtung seitens der NCP engineering GmbH dar. Änderungen zum Zwecke des technischen Fortschritts bleiben der NCP engineering GmbH vorbehalten.

Warenzeichen

Alle genannten Produkte sind eingetragene Warenzeichen der jeweiligen Urheber.

Stand April 2016

Next Generation Network
Access Technology

www.ncp-e.com