miho Inspektionssysteme GmbH
Obervellmarsche Str. 12
34292 Ahnatal
Tel: +49/5609/8382-0
Fax: +49/5609/6168
Mail: info@miho.de
www.miho.de

miho IT-Richtlinien

Stand 2018-01-30

Einleitung

Erfolgreiche Fernwartung ist der Schlüssel zu mehr Kundenzufriedenheit durch Kostenminimierung und geringere Maschinenstillstandszeiten, schont aber auch die Ressourcen des jeweiligen Maschinenherstellers.

Früher wurden die fernzuwartenden Maschinen bevorzugt mittels Modem-Technologie über das weltweit verfügbare Telefonnetz erreicht. Dabei kamen im Normalfall analoge Modems zum Einsatz (eben wegen der weltweiten Verbreitung des analogen Telefonnetzes) – in Einzelfällen aber auch ISDN-basierte Lösungen.

Neben den Vorteilen der Anbindung mittels Modem

- Analoges Telefonnetz (noch nahezu) weltweit verfügbar, notfalls über Mobile Telefonnetze
- Geringe Sicherheitsrisiken durch direkte, leitungsvermittelte Punkt-zu-Punkt-Verbindung hat diese aber auch - teils gravierende – Nachteile:
- Große Instabilitäten der aufgebauten Verbindungen (erfordern häufig neuen Verbindungsaufbau)
- Geringe erreichbare Geschwindigkeiten (häufig unter 19000 Bit/s)
- Mögliche Probleme durch kundenseitige Umstellung auf neue Technologien (wie etwa VOIP)
- Gesonderte Infrastruktur (Kabel/ Anbindung an die TK-Anlage, …) erforderlich

Insbesondere bei der Fernwartung von komplexeren Bildverarbeitungssystemen hat sich die geringe Geschwindigkeit der Modem-Verbindung zu einem KO-Kriterium entwickelt, da der hierdurch bedingte langsame Bildaufbau am Rechner des durchführenden Servicetechnikers eine hinreichend flüssige Bedienung der Maschine nicht mehr ermöglicht.

Als Alternative haben sich internetbasierte Technologien als Standard etabliert, mit folgenden Vorteilen:

- Ähnlich weit verbreitet wie das Telefonnetz
- Universelles und ausbaubares Netzwerk, sehr ausfallsicher
- Gefahr von Verbindungsabbrüchen praktisch nicht vorhanden
- Geschwindigkeit ist skalierbar und häufig nur eine Preisfrage
- Flexibilität: Verbindung kann durch das bereits vorhandene Netzwerk des Kunden geleitet werden, es kann aber ebenso ein autarker Zugang eingerichtet werden bei ähnlicher Einfachheit wie die eines Modemanschlusses

Allerdings sind auch folgende Nachteile zu beachten:

- Sicherheit:
  Durch das Internet geleitete Informationen werden prinzipbedingt über ungesicherte und teils anonyme Verbindungswege geleitet. Deshalb ist eine Verschlüsselung der übermittelten Daten/Informationen obligatorisch.
  Daneben gilt es zu verhindern, dass unautorisierte Personen Zugang zur Maschine des Kunden erhalten. Hierfür müssen geeignete Methoden zur Authentifizierung des Servicetechnikers - aber auch der kundenseitigen Maschine - gewählt werden.
- Die zugrundeliegende Netzwerktechnologie setzt ein deutlich höheres Fachwissen zu deren Beherrschung voraus.

Zum Thema Sicherheit sollte prinzipiell angemerkt werden, dass es keine 100%ige Sicherheit gibt, ja geben kann – weder mit Modemanbindung, noch über das Internet, noch ganz ohne externe Anbindung. Wenn ein Zugriff auf eine Maschine gewünscht wird, kann er erfolgen – und sei es durch Ausnutzung des schwächsten Gliedes vor Ort, z.B. durch Bestechung eines Mitarbeiters. Letztlich ist es eine Frage der Einschätzung des Risikos und der adäquat verwendeten Hürden, die man einem potentiellen Angreifer in den Weg legt.

Zusammengefasst lässt sich sagen, dass die Vorteile der Internetbasierten Fernwartung spätestens für komplexere Systeme wie die der Bildverarbeitung deutlich überwiegen, man aber die richtige Absicherung dieses Mediums umsetzen muss.

Technische Umsetzung

Für die Verschlüsselung und die Authentifizierung wird das Programmpaket OpenVPN gewählt.

Es bietet folgende entscheidende Vorteile:

- Authentifizierung dem Stand der Technik entsprechend über ein „public key“ Verfahren
- Modulare, als sicher geltende, Verschlüsselung der übertragenen Daten
- Komplette Kommunikation über einen Port
- NAT-fähig
- Leicht über Netzwerke zu routen
- Erfahrungen im Hause miho über Jahre vorhanden, da zur eigenen Fernwartung im Einsatz

Die praktische Implementierung sieht so aus, dass im Hause miho ein ausschließlich für Fernwartung bestimmter Server eingerichtet wurde (RA1), der internetseitig und firmenseitig jeweils durch Firewalls gesichert ist.

Zu diesem Fernwartungsserver baut nun der Kunde bei Bedarf einen VPN-Tunnel auf. D. h. es besteht nun, ausgelöst durch den Kunden, eine Punkt-zu-Punkt-Verbindung zwischen der kundenseitigen Maschine und unserem Fernwartungsserver. Dabei erhält jede einzelne Maschine ein eigenes Zertifikat, mit dem sie sich unserem Fernwartungsserver gegenüber ausweist. Bei Missbrauch kann dieses Zertifikat sehr leicht in unserem Hause zurückgezogen werden, wodurch ein weiterer Zugriff auf den Fernwartungsserver verhindert wird.

Gleichzeitig erhält ein Servicetechniker unseres Hauses nach Eingang des Fernwartungsauftrages die Möglichkeit, ebenso einen VPN-Tunnel von seinem Arbeitsplatz (bei Bedarf weltweit!) zum Fernwartungsserver aufzubauen. Hierdurch „klinkt“ er sich in das gleiche virtuell private Netzwerk (VPN) ein, indem sich die Kundenmaschine schon befindet und kann mit der Fernwartung beginnen.

Natürlich muss sich auch der Servicetechniker mit einem entsprechenden Zertifikat authentifizieren.

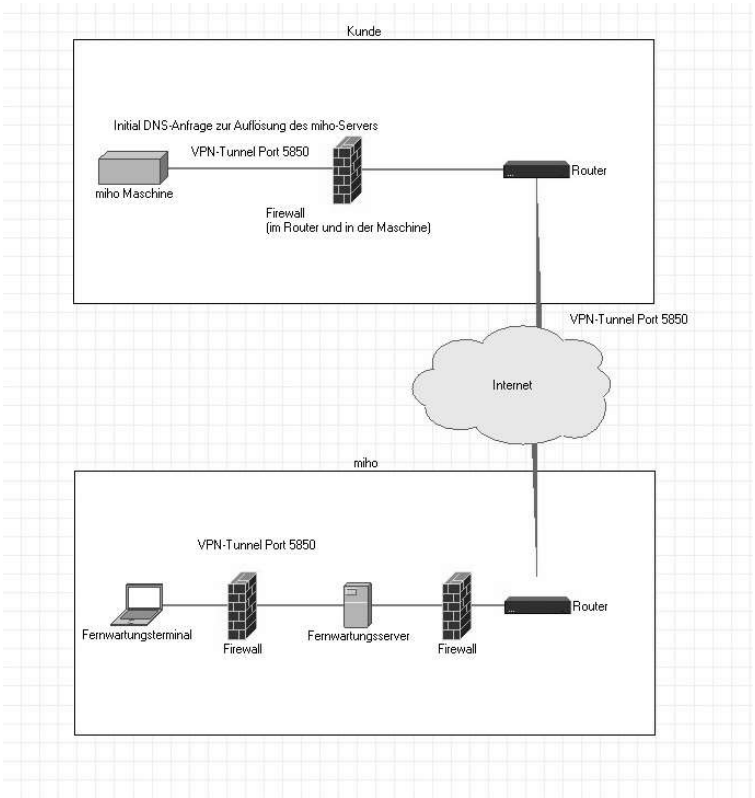
Der Fernwartungsserver hat eine dynamisch aufgelöste Adresse im Internet, was eine weitere Hürde gegen einen Angriff darstellt.

Die Kundenmaschine erfragt zunächst via DNS-Abfrage (Port 53 UDP oder TCP) die Adresse des miho-Fernwartungsservers (ra1-miho.dyndns.org, ra1-miho.ignorelist.com).

Zwar existiert auch eine statische Adresse (94.79.148.178), diese sollte jedoch nicht verwendet werden, da sie bei einem eventuellen Wechsel des Internetproviders nicht mehr gültig wäre!

Anschließend wird die verschlüsselte Kommunikation durch Kontaktierung des Fernwartungsservers über Port 5850 (UDP) initiiert. Die eigentliche verschlüsselte Kommunikation erfolgt dann über eine Socket-Verbindung mit Client-seitig dynamisch zugewiesener Portnummer (wie üblich bei Socket-Verbindungen). Bedingt durch die Tatsache, dass die Kundenmaschine die Verbindung initiiert, muss bei einfachen Strukturen (Kunde hat für die Maschine einen DSL-Anschluss geschaltet) noch nicht einmal eine Portweiterleitung in der kundenseitigen Firewall (hier: im DSL-Router und in der miho-Maschine) eingerichtet werden.

Beispielkonfiguration:



Technische Voraussetzungen

Möglichkeit 1 – Stand-alone:

Separater Internet (DSL) Anschluss für miho Geräte

Möglichkeit 2 – Integration in bestehendes IT System:

Separates Netzwerk mit Zugriff auf das Internet über Ports 53 (TCP&UDP) & 5850 (UDP) für die Etablierung der Socket-Verbindung zum Fernwartungsserver auf Client-seitig dynamisch zugewiesenem Port. Es werden pro miho Gerät eine IP Adresse zuzüglich einer Reserve IP Adresse für Servicezwecke aus diesem Netzwerk benötigt.

Für Upgradeaktionen muss zusätzlich auch noch der Port 5851 (UDP) ausgehend (und der Client-seitig dynamisch zugewiesene Port eingehend) freigegeben sein.

Alternative: Teamviewer

Hat ein Kunde bereits eine Teamviewer-Lizenz, kann auch diese für unsere Fernwartung eingesetzt werden. Wir weisen aber darauf hin, dass unsere auf OpenVPN basierte Lösung die bei unseren Kunden verbreitetste und damit am besten unterstützte Lösung darstellt und dass bei der Verwendung von Teamviewer Datenverkehr teils über Server der Fa. Teamviewer geleitet wird, für deren Sicherheit wir keine Gewährleistung übernehmen können (proprietäre Software).

Administratorzugang für Kunden

Der Administratorzugang für miho Maschinen und PCs ist normalerweise dem Kunden nicht zugänglich, um Fehlkonfigurationen und damit verbundene Geräte- und Produktionsausfälle zu vermeiden.

Außerdem wird damit sichergestellt, dass nicht durch die Installation von Fremdsoftware Viren oder andere Schadsoftware auf miho-Geräte oder gar das kundenseitige Netz gelangen können.

Wünscht der Kunde explizit die Herausgabe der Administratorkennung von miho-Geräten oder PCs, kann dies gegen Unterschrift dieser Erklärung und der damit verbundenen Haftungsfreistellung erfolgen.

In diesem Fall kann miho aber keinerlei Verantwortung für Schäden, die mittelbar oder unmittelbar durch die kundenseitige Nutzung der Administratorkonten entstanden sind übernehmen, explizit also z. B.:

- Datenverluste,
- Produktionsausfälle
- Ausbreitung von Viren oder anderer Schadsoftware,
- auftretende Softwareinkompatibilitäten.

Wir verstehen o. g. Ausführungen und erklären hiermit, dass die Herausgabe der Administratorzugänge der miho-Geräte und PCs auf eigenen Wunsch und unter ausdrücklicher Inkaufnahme der genannten Risiken gewünscht wird.

Die Fa. miho Inspektionssysteme GmbH stellt sich von jeglicher Verantwortung und möglichen Schadenersatzforderungen für oben genannte Fälle frei.

Fernwartung

Die Fernwartung der durch miho gefertigten Maschinen und Geräte wird aus Sicherheitsgründen normalerweise nur über folgende Mittel ausgeführt:

1. direkte Wählverbindung (Kunde stellt eine analoge Telefonleitung)

2. direkte Ankopplung über einen eigenen Internetzugang (Kunde stellt geeigneten Internetzugang zur Verfügung)

Beiden Anbindungsarten ist gemeinsam, dass jegliche Verbindung zum kundenseitigen Netzwerk vermieden wird.

Damit wird sichergestellt, dass weder Viren oder andere Schadsoftware von miho-Geräten das kundenseitige Netz stören können, noch umgekehrt o.g. Software Einfluss auf miho Geräte nehmen kann.

Wünscht der Kunde explizit eine Anbindung der miho-Geräte in seine Netzwerkinfrastruktur, kann dies technisch umgesetzt werden.

In diesem Fall kann miho aber keinerlei Verantwortung für Schäden, die mittelbar oder unmittelbar durch die Vernetzung entstanden sind übernehmen, explizit also z. B.:

- Datenverluste,
- Produktionsausfälle

durch die Ausbreitung durch Viren oder anderer Schadsoftware oder auch nur durch Softwareinkompatibilitäten.

Wir verstehen o .g. Ausführungen und erklären hiermit, dass die Vernetzung der miho-Geräte auf eigenen Wunsch und unter ausdrücklicher Inkaufnahme der genannten Risiken gewünscht wird.

Die Fa. miho Inspektionssysteme GmbH stellt sich von jeglicher Verantwortung und möglichen Schadenersatzforderungen für oben genannte Fälle frei.

Betriebsdatenerfassung

Die Übermittlung von Betriebsdaten der durch miho gefertigten Maschinen und Geräte wird aus Sicherheitsgründen generell nur über folgendes Mittel ausgeführt:

- direkte Ankopplung eines Auswertesystems (PC) über eine eigene Netzwerkverbindung.

So wird jegliche Verbindung zum kundenseitigen Netzwerk vermieden.

Damit wird sichergestellt, dass weder Viren oder andere Schadsoftware von miho-Geräten das kundenseitige Netz stören können, noch umgekehrt o.g. Software Einfluss auf miho-Geräte nehmen kann.

Wünscht der Kunde explizit eine Anbindung der miho-Geräte, kann dies technisch umgesetzt werden.

Voraussetzung ist, dass der Kunde auf der Strecke zwischen miho-Gerät und BDE eine minimale Bandbreite von 256 Kbps für die Socketverbindung der BDE garantiert (Port 50.000 TCP).

Die Abfragedauer über einen ggf. über ein WAN abgesetzten Viewer ist stark von der zur Verfügung stehenden Bandbreite abhängig. Es wird eine Bandbreite von mindestens 4 Mbps gefordert und eine Bandbreite von 10 Mbps dringend empfohlen!

In diesem Fall kann miho aber keinerlei Verantwortung für Schäden, die mittelbar oder unmittelbar durch die Vernetzung entstanden sind übernehmen, explizit also z. B.:

- Datenverluste,
- Produktionsausfälle

durch die Ausbreitung durch Viren oder anderer Schadsoftware oder auch nur durch Softwareinkompatibilitäten.

Die Firma miho garantiert, daß die gelieferten Maschinen und Geräte zum Zeitpunkt der Auslieferung frei von Viren und anderer Schadsoftware sind. Da die Geräte für Wartungspersonal etc. zugänglich sind, kann miho zu einem späteren Zeitpunkt hierfür keine Garantie übernehmen.

Wir verstehen o .g. Ausführungen und erklären hiermit, dass die Vernetzung der miho-Geräte auf eigenen Wunsch und unter ausdrücklicher Inkaufnahme der genannten Risiken gewünscht wird.

Die Fa. miho Inspektionssysteme GmbH stellt sich von jeglicher Verantwortung und möglichen Schadenersatzforderungen für oben genannte Fälle frei.

Vorbedingungen für Installation und Wartung

Sowohl für die Installation der verschiedenen Softwarekomponenten für die Fernwartung, als auch der Betriebsdatenerfassung benötigen wir lokale Administratorkonten.

Insbesondere bei Integration in das Kundennetzwerk muss der Kunde sicherstellen, dass zu den vereinbarten Installationszeiten ein Mitarbeiter seiner IT-Abteilung zur reibungslosen Abwicklung der notwendigen Integrationsarbeiten zur Verfügung steht.