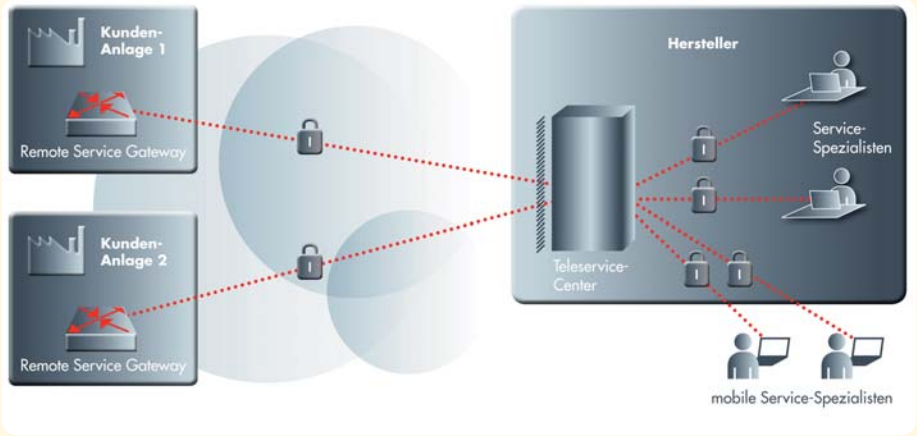

Bild 1: Zugangsverwaltung der Fernwartung – schematische Darstellung

Intelligente Zugangsverwaltung

Was tun, wenn der Wartungsmitarbeiter geht?

Anlagenhersteller müssen Service bieten, auch lange über die Gewährleistungszeit hinaus. Heutzutage ist es selbstverständlich, dass Teile dieses Services nicht vor Ort, sondern als Fernwartung erbracht werden, um Zeit und Kosten zu sparen. Bei heutigen Fernwartungslösungen haben Wartungsmitarbeiter meist eine direkte Verbindung zu den Anlagen. Sie müssen die Zugangswege und -parameter zu allen Anlagen kennen, die in Wartung sind, seien es Telefonnummer und Login bei Modemlösungen oder VPN-Parameter bei Internetwartung. Wie aber werden die Zugänge verwaltet, um Änderungen schnell bekannt zu machen? Und noch wichtiger: Was passiert, wenn ein Wartungsmitarbeiter gekündigt wird oder von sich aus zum Mitbewerb wechselt? Der Zugang zu den Anlagen kann effektiv geregelt werden.

Am einfachsten ist die Verwaltung noch für Virtuelle Private Netze (VPNs) mit individuellen Mitarbeiterzugängen. Hier muss der Betreiber 'nur' den Login zu allen Anlagen manuell sperren, was je nach Anzahl bereits zu einem erheblichen Aufwand führen kann. Schwieriger ist es bei VPNs mit einem gemeinsamen Login für alle Mitarbeiter oder bei Modemzugängen, die im Normalfall nur einen einzigen Wartungslogin verwenden. Hier muss der Hersteller nicht nur die Zugänge zu allen Anlagen ändern, sondern auch allen Wartungsmitarbeitern die geänderten Zugangsdaten mitteilen. Während dieser Zeit hat ein gekündigter Mitarbeiter weiterhin vollen Zugriff auf alle Anlagen. Dieser hohe Aufwand führt außerdem oft dazu, dass Hersteller einmal vergebene Wartungszugänge während der gesamten Laufzeit einer Anlage unverändert lassen. Das ist sowohl aus Hersteller- wie auch aus Kundensicht ungünstig. Die Lösung dieses Dilemmas ist einfach: Wartungsmitarbeiter bekommen keinen direkten Zugang zu den Anlagen mehr. Stattdessen öffnet ihnen ein virtueller Pförtner in der Zentrale den Zugang nur bei Bedarf. Dieser Pförtner ist wie sein realer Gegenpart der einzige, der über alle Zugänge verfügt. Verlässt ein Wartungsmitarbeiter das Unternehmen, sperrt der Pförtner seinen Zugang zur Zentrale und damit automatisch auch zu allen Anlagen. Ändern sich die Logins zu einer Anlage oder sogar die Art der Anlagenanbindung, ist das für die Mitarbeiter nicht von Interesse. Für den Service Fernwartung muss nur der Pförtner diese Information haben.

Intelligentes Verbindungsmanagement

Aus technischer Sicht ist ein solcher virtueller Pförtner ein Rechner unter Kontrolle des Anlagenherstellers, der einen zentralen

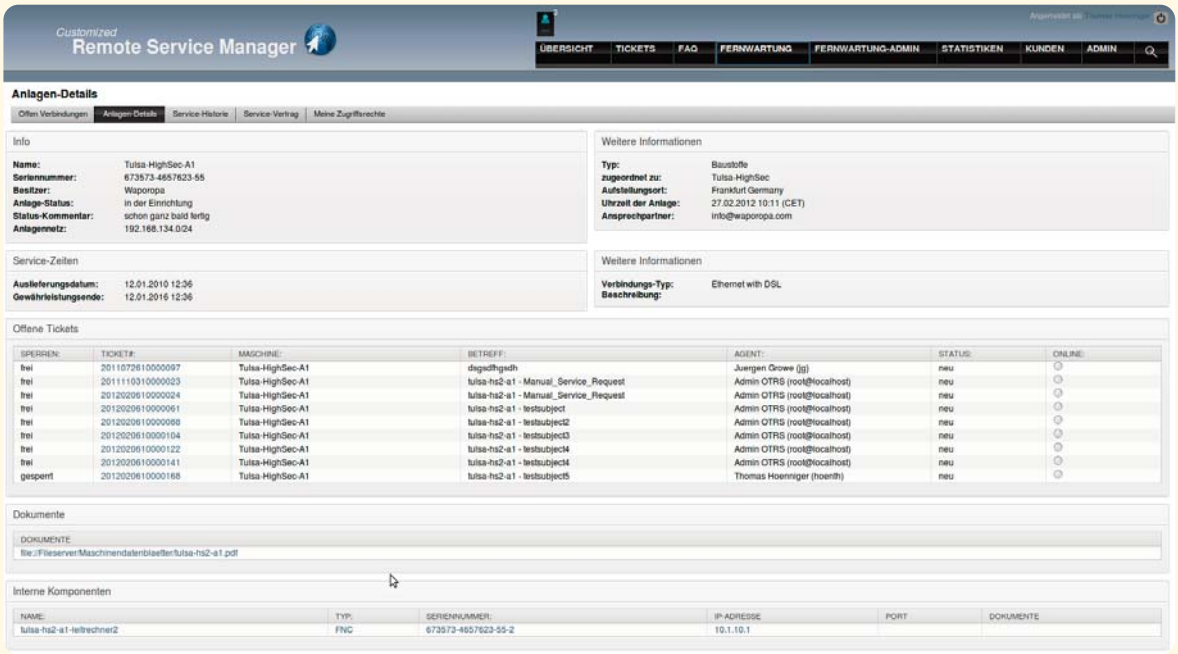

Bild 2: Detailansicht einer CRSM verwalteten Anlage mit offenen Wartungstickets

Dienst zum Verbindungsmanagement anbietet. Auf der einen Seite verwaltet er die gewarteten Anlagen: Der Verbindungsmanager benötigt Zugangsparameter und Informationen über die Art der Anbindung, sei es per Internet, Modemverbindung oder Sonderlösungen. Dabei kommen zwischen Verbindungsmanager und Anlage anbindungsspezifische Module zum Einsatz. So können alle heutigen und auch zukünftig denkbare Techniken abgebildet werden. Idealerweise abstrahiert der Verbindungsmanager auch gleich die Art der Anlagenanbindung. Jede Anlage ist auf dieselbe Weise erreichbar, die Verbindung ist einfach 'da'. Für Wartungszwecke sehen dann alle Anbindungen gleich aus, lediglich die Übertragungsgeschwindigkeiten sind unterschiedlich. Sind alle Parameter bekannt, wird eine verschlüsselte Verbindung zwischen Anlage und Verbindungsmanager geöffnet. Diese kann sowohl permanent, als auch nur nach Kundenaufforderung aktiv sein. Daneben müssen die Wartungsmitarbeiter verwaltet werden: Sie verbinden sich über geeignete VPN-Techniken mit dem Verbindungsmanager. Von dort können sie schon aktive Verbindungen zu den Anlagen nutzen oder aber neue Verbindungen initiieren, auch ohne die Login-Parameter selbst zu kennen. Die dazu nötige Logik steckt im Verbindungsmanagement-Dienst.

Der Zugang zum Verbindungsmanager reicht aus. An diesem Punkt ist ein leistungsfähiges Rechtekonzept nötig, um möglichen Missbrauch auszuschließen. Glücklicherweise kann das einfach realisiert werden: Die verschlüsselten Verbindungen führen jetzt nicht mehr direkt von den Wartungsmitarbeitern zu den Anlagen, sondern werden im Verbindungsmanager aufgebrochen. Hier können erlaubte Zugriffe also leicht dynamisch verschaltet werden. Alle anderen Zugriffe sind implizit verboten.

Aus dem Konzept eines zentralen Pförtners ergeben sich einige Vorteile:

- Alle Kennungen (Anlagen und Mitarbeiter) werden zentral von geschulten Mitarbeitern verwaltet.
- Beim Weggang eines Mitarbeiters muss lediglich dessen Berechtigung zum Zugriff auf den Verbindungsmanager gelöscht werden. Mehr ist nicht nötig. Da der Mitarbeiter nie Kenntnis von weiteren Parametern hatte, müssen diese auch nicht geändert werden.
- Ändern sich Zugangsparameter oder Anbindung einer Anlage oder kommen neue Anlagen dazu, müssen die Daten nur an einer Stelle gepflegt werden.
- Es kann zentral dokumentiert werden, wann Anlagen gewartet wurden und wie lange der Vorgang dauerte. Die gespeicherten Daten können direkt für die Abrechnung oder zum Nachweis der Einhaltung von Service Level Agreements verwendet werden.
- Ein Wartungsmitarbeiter kann problemlos an mehreren Anlagen gleichzeitig arbeiten, oder mehrere Mitarbeiter an einer Anlage.
- Es lassen sich an zentraler Stelle sehr fein einstellbare Rechte definieren, bis hinunter zu einzelnen Diensten auf einzelnen Rechnern einer Anlage.
- Endkunden können den Zugriff auf 'ihre' Anlage über ein Kundenportal selbst bestimmen und die Wartungshistorie ihrer Anlagen einsehen.
- Erweiterungen wie ein Servicedesk, Ticketsystem oder proaktives Maschinen-Monitoring sind an zentraler Stelle einfach zu implementieren.

Im Hinblick auf die immer größer und komplexer werdenden Anlagen, der steigenden Beteiligung von Zulieferern an der Wartung und dem wachsenden Sicherheitsbedürfnis der Endkunden ist der Schritt zu einer zentralen Verwaltung aller Fernwartungszugänge inzwischen überfällig. Die ersten derartigen Produkte, wie der Customized Remote Service Manager (CRSM) der HighConsulting sind inzwischen verfügbar. ■

www.high-consulting.de

Autor: Dr. Walter Hafner, Geschäftsführer der HighConsulting GmbH & Co. KG