Bild: HighConsulting GmbH & Co. KG

Bild 1: Flexibel und leistungsfähig: Die Fernwartung von Anlagen über ein Portal. Der Customized Remote Service Manager (CRSM) von HighConsulting erlaubt die modulare Integration beliebiger Anbindungen.

Immer die beste Lösung?

Portale in der Cloud

Die Cloud als Allheilmittel für alle IT-Probleme? Mit der Cloud wird alles viel einfacher? Das und Ähnliches suggerieren derzeit viele Hersteller und sogar manche Fachzeitschriften. Um es vorwegzunehmen: Ja, die Cloud kann eine hilfreiche Komponente in der IT-Infrastruktur eines Unternehmens sein, um bestimmte Prozesse zu vereinfachen. Doch sind Cloud-basierte Portale auch die optimale Lösung für eine Fernwartung von Systemen? Oder anders gefragt: Wann sollten Unternehmen doch besser auf das klassische Rechenzentrum setzen?

Zur Veranschaulichung ein fiktives Beispiel: Die Max Mischer AG entwickelt Anlagen zur Zementproduktion und vertreibt diese weltweit. Da die Anlagen wartungsintensiv sind, setzt das Unternehmen schon lange auf die Fernwartung. Zunächst kamen Modem- und ISDN-Lösungen mit einer Direktverbindung zum Einsatz, nach Kundenvorgaben wird aber neuerdings auch verschlüsselt per VPN über das Internet gewartet. Mit wachsender Anzahl der zu wartenden Anlagen und damit verbunden der Anzahl an Technikern, wurde das fehlende Rechte- und Verbindungsmanagement immer mehr zum Problem. Eine neue Lösung musste also gefunden werden. Die flexibelste und leistungsfähigste Technik zur Fernwartung von Anlagen ist aktuell das Portal: Der Zugriff erfolgt hier webbasiert und ist weltweit verschlüsselt möglich. Das Rechte- und Verbindungsmanagement wird dabei an einem Ort gebündelt. Sowohl der Zugang der Techniker als auch die Dokumentation ihrer Leistung wird zentral verwaltet. In der Summe haben Portallösungen zahlreiche unschlagbare Vorteile. Auch die Max Mischer AG entscheidet sich daher für eine Portallösung. Um möglichst wenig interne Ressourcen zu binden und keine eigene Hardware finanzieren und administrieren zu müssen, bevorzugt das Unternehmen den Betrieb in der Cloud. Updates können dann problemlos vom Dienstleister eingespielt werden, eine Verfügbarkeitsgarantie sichert die Performance. Doch im Licht der NSA-Berichte bleiben natürlich Zweifel, ob trotz Verschlüsselung der Daten deren Vertraulichkeit in der Cloud ausreichend geschützt ist. Je nach Sicherheitsanforderungen lassen sich auch hierfür Lösungen finden, beispielsweise durch den zugesicherten Betrieb in einem deutschen Rechenzentrum. Dass auch in diesem Fall interne Daten das Unternehmen verlassen und ohne Kontrollmöglichkeit extern gespeichert werden, muss jedoch in Kauf genommen werden.

Wo steht das Portal?

Bald aber wird der Max Mischer AG eine neue Hürde bewusst: Cloud-Lösungen unterstützen nicht jede beliebige Anbindung einer Anlage. Bei einer großen Anzahl installierter Systeme wird das zum ernsten Problem werden.

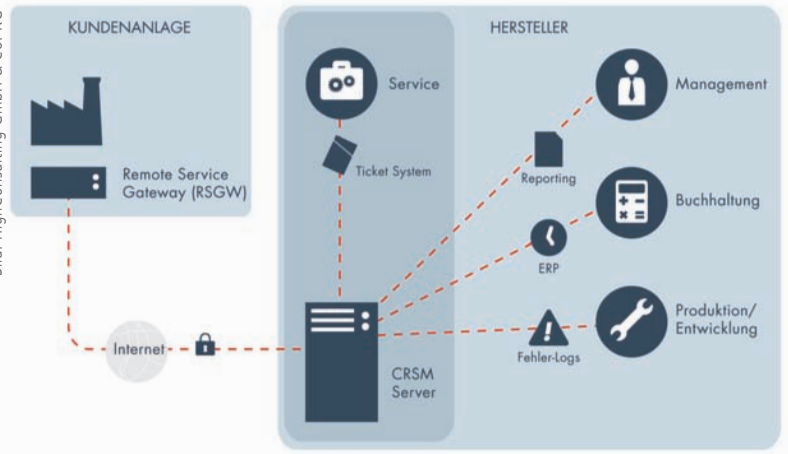

Bild: HighConsulting GmbH & Co. KG

Bild 2: Portal ist nicht gleich Portal. Steht der Portalserver beim Hersteller, ist eine viel engere Unternehmensintegration möglich als bei Cloud-Portalen.

Wie lassen sich die alten Modems in Anlagen am Ende der Welt durch VPN-Router ersetzen? Werden alle Endkunden der Umstellung ihrer Anbindung zustimmen? Und wer übernimmt die Kosten? Wenn alle bestehenden Anlagen ausnahmslos über die neue Portallösung gewartet werden sollen, müssen entweder die alten Anlagen auf die neue Technik umgestellt werden oder aber ältere Modem- und ISDN-Verbindungen in die neue Portallösung integriert werden. Während die Umstellung auf VPN einen großen organisatorischen und finanziellen Aufwand bedeutet, erfordert die Integration der alten Technik den Betrieb des Portals in Eigenregie, da hierfür sowohl die Software angepasst werden muss als auch weitere Hardware erforderlich ist. Einen Königsweg gibt es da leider nicht. In der Regel gilt jedoch: Je höher die Anzahl der existierenden Anlagen und je vielfältiger die eingesetzten Anbindungstechniken sind, desto sinnvoller und kosteneffizienter ist die Einbindung der bestehenden Infrastruktur in das Portal. Unter dieser Voraussetzung entscheidet sich auch die Max Mischer AG für die Einbindung der bestehenden, alten Technik in ein modernes Portal, das im eigenen Rechenzentrum betrieben wird. Eine passende Lösung, die eine modularisierte Integration beliebiger Anbindungen erlaubt, ist z.B. der Customized Remote Service Manager (CRSM) von HighConsulting.

Höherer Mehrwert

Einmal installiert stellt sich schnell heraus, dass der Betrieb eines Portals im eigenen Haus weitere Vorteile bringt: In dasselbe Netz wie die unternehmensinternen IT-Systeme eingebunden, kann die Fernwartung eng mit den Unternehmensabläufen verzahnt werden. An das Portal lassen sich problemlos Ticket-Systeme anbinden, Berechtigungen zur Fernwartung können durch Fehlertickets erteilt werden und Auswertungen werden systemübergreifend mit der Konstruktionsabteilung abgeglichen. Eine Kopplung mit der Vertriebs-Datenbank oder einem ERP-System erlaubt den Zugriff auf Kunden- und Anlagen-Stammdaten. Eine Anbindung ans Rechnungswesen gewährleistet eine lückenlose Abrechnung der Wartungstätigkeiten. Viele Unternehmensabläufe lassen sich – je nach Unterstützung durch die Fernwartungssoftware – sehr detailliert modellieren. Nach den Erfahrungen der HighConsulting sollte das auch angestrebt werden, da dies einerseits die Akzeptanz der Software durch die Mitarbeiter erhöht und andererseits die Produktivität steigt, wenn Ergebnisse der Fernwartung auch anderen Abteilungen zur Verfügung stehen. Ein Portal-Betrieb in Eigenregie kann bei fehlerhaftem Konzept ein höheres Ausfallrisiko bedeuten. Fällt die Entscheidung für eine Cloud-Lösung, sollte daher unbedingt darauf geachtet werden, dass der Betreiber für redundante Systeme sorgt, Backups anlegt, Desaster-Recovery-Pläne hat und eventuell sogar Server in mehreren Rechenzentren betreibt. Wer sein Portal dagegen im eigenen Rechenzentrum betreibt, ist für die Sicherheit selbst verantwortlich. Eine Server-Virtualisierung allein ist selten ausreichend, die größte Sicherheit bringt nur der simultane Betrieb mehrerer Fernwartungsserver in einem Verbund. Sollte einmal ein Server ausfallen, verbinden sich Anlagen und Anwender automatisch mit einem anderen Server. Geplante Wartungszeiten, etwa für Updates, lassen sich damit ohne Ausfall einhalten. Der Betrieb eines Server-Verbunds hat aber noch weitere Vorteile. Ein Verbund im Rechenzentrum sichert gegen Ausfälle ab. Wird der Verbund aber weltweit auf Servern verteilt, verbessert sich auch die Qualität der Fernwartung enorm. Durch einen Server-Verbund können Anlagen in restriktiven Ländern wie beispielsweise China von Technikern einer lokalen Niederlassung ohne Umwege gewartet werden und auch staatliche Firewalls sind dann kein Thema mehr. Für den notwendigen Datenabgleich reicht dann eine schmalbandige, nur bei Bedarf geschaltete Verbindung aus. Ein weltweit agierendes Unternehmen kommt so ohne Umstellung der bisherigen Fernwartungsstrukturen zu einer modernen, leistungsfähigen Portallösung und genießt zudem noch alle Vorteile, die eine enge Einbindung in das Unternehmen mit sich bringt.

Fazit

Generell ist die Fernwartung über ein Cloud-Portal für alle Unternehmen sinnvoll, die bis jetzt noch keine Fernwartung anbieten und die davon ausgehen, ihre Anlagen künftig mit einer standardisierten Technik anbinden zu können. Unternehmen, für die eine Umstellung ihrer Fernwartung zu aufwendig oder sogar unmöglich ist, sollten ihre Fernwartungslösung selbst betreiben und bestehende Techniken dort einbinden. Auch Unternehmen, denen die Anpassung der Fernwartung an ihre eigenen Unternehmensabläufe wichtig ist, sollten der Serverlösung den Vorzug geben. Und solange keine Hardware-Erweiterungen zur Einbindung in das Portal notwendig sind, spricht nichts dagegen, ein Fernwartungs-Portal wie den HighConsulting CRSM bei einem Cloud-Dienstleister zu betreiben. ■

www.high-consulting.de

Autor: Dr. Walter Hafner, Geschäftsführer, High Consulting GmbH & Co. KG

Auszug aus dem SPS-MAGAZIN, Fachzeitschrift für Automatisierungstechnik, Ausgabe 4/2014.