Internet-Gateway mit hohem Sicherheitsstandard

‚Virtual Private Infrastructure' für die Fernwartung per Internet

Das Thema ‚Embedded Internet' ist im Moment ein Modethema. Kaum eine Firma hat heute nicht irgend ein Produkt im Sortiment, das auch unter der Internet-Fahne segelt. Schaut man sich die Produkte einerseits und die geweckten Wünsche und Anforderungen andererseits etwas genauer an, so muss man feststellen, dass hier eine große Lücke klafft. Wie bei fast allen Technologieströmungen wird auf die euphorische Phase eine Ernüchterungsphase folgen, die solange dauert, bis sich der Graben zwischen Anforderungen und Realität einigermaßen geschlossen hat. Anhand eines Beispiels aus der Wirtschaft werden die auftretenden Sicherheitsprobleme exemplarisch aufgearbeitet und aufgezeigt, wie wichtig ein ganzheitlicher Ansatz und eine konsequente Architektur für dieses Thema sind.

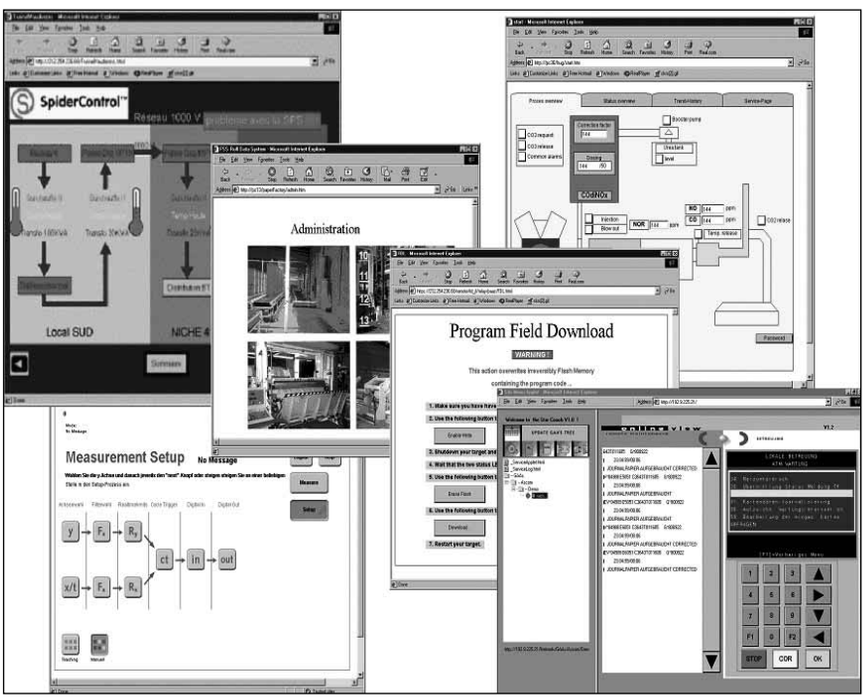

Abb. 1: Direkter Zugriff mit einem handelsüblichen Browser auf die Bedienung der Maschine

Vorteile der Webtechnologie

‚Was bringt mir Webtechnologie, was ich nicht heute schon besser lösen kann?' Diese Kritik wird von verschiedener Seite immer wieder vorgebracht. Tatsächlich kann die Internettechnologie ein paar Dinge, die bisher in dieser Form nicht möglich waren. Der wichtigste Vorteil besteht darin, dass man mit einem guten Gesamtkonzept mit Hilfe von Webtechnologien viel Geld sparen kann. Einsparungen lassen sich bei der Software-Entwicklung und durch veränderte Service- und Unterhaltskonzepte erzielen. Die Ursachen für dieses Einsparungspotenzial sind vielfältig und bei jedem Projekt wieder etwas anders gelagert. Wichtige Punkte sind: Die Webtechnologie kann auf bereits bestehenden Ressourcen (Netzwerke) aufsetzen, sie vereinigt die Standards von Büroinformatik und Automation, ermöglicht flexiblere Lösungen und ist skalierbar. Dadurch ergibt sich eine gesicherte Investition:

- Bessere Wartbarkeit
- Plattformunabhängigkeit
- Größere Zukunftssicherheit

Autoren

Dr. MATTHIAS BAUMGARTNER und PETER BRÜGGER gehören zur Geschäftsleitung der iniNet AG;
Seewenweg 5, CH-4153 Reinach
Fon: +41/61/71696-26, Fax: +41/61/71696-17
E-Mail: info@ininet.ch

Vermeidung von Investitionsruinen

Der Schlüssel zur Erschließung des enormen Potenzials dieser Technologien liegt in einem guten Gesamtkonzept. Wir möchten nun versuchen, eine verallgemeinerte Sicht der Problematik ‚Fernwartung per Internet' zu entwickeln.

Design

Von ihrer Natur her müssen Systeme, die Embedded-Webtechnologie einsetzen, von Anfang an als verteilte Systeme aufgefasst werden. Sun Microsystems prägte das Schlagwort ‚The Network is the Computer', und dies gilt umso mehr für das Embedded-Umfeld, wo die Granularität der Systeme nochmals wesentlich feiner ist, wie im Internet-typischen Client-Server-Umfeld. Diese Aussage bedeutet, dass man nicht zuerst Insellösungen programmieren darf, die danach noch vernetzt werden. Vielmehr sollte von Anfang an ein Gesamtsystem definiert werden, das anschließend auf die real existierenden Netzwerkressourcen verteilt wird. Es gilt, einen objektorientierten Ansatz konsequent weiter zu denken und sich diese Objekte in einem vernetzten Umfeld vorzustellen. Es ist darum unerlässlich, von Anfang an ein gutes und stabiles Konzept zu definieren. Das heißt, es sollten gleich alle möglichen Anforderungen in das Konzept mit einfließen.

Internetanbindung

Eine typische Anforderung dieser Art ist die Internetanbindung. Bei genauerer Betrachtung stellt sich heraus, dass es nicht einfach darum geht, irgendwie eine Verbindung ans Netz zu realisieren. Die Internetanbindung ist eine multifunktionale Schnittstelle zur Welt, d.h. es werden die verschiedensten Dienste, Zugänge und Informationen über dieses Interface angeboten. Darunter fallen:

- Fernwartung einzelner Maschinen durch den Hersteller (Troubleshooting, Firmware Updates)
- Wartungs- und Servicearbeiten für extern vergebene Dienstleister (Outsourcing)
- Sicherheits- und Alarmierungsfunktionen
- Informationsbeschaffung für das Supply Chain Management
- Enterprise Ressource Planning
- Zugriff für eigene, extern arbeitende Mitarbeiter
- Zugriff für Freelancer

Wird überlegt, welche Tätigkeiten diese Personen ausführen könnten und welche Geräte und Maschinen dafür in Frage kommen, ergibt sich folgendes Bild: Viele Geräte sind heute schon mit einem Embedded-Webserver ausgerüstet. Andere können über einen Add-On-Server nachgerüstet werden oder sind als Gruppe auf ein webserverfähiges System abgebildet. Einige dieser Konzepte werden bereits fertig mit dem Gerät ausgeliefert und können nicht geändert werden, andere Webanbindungen werden vom Systemintegrator selber gemacht. Die Aufgabe besteht darin, alle diese Systeme mit dem Internet zu verbinden, so dass die verschiedenen Benutzergruppen selektiv auf ‚ihre' Systeme zugreifen können. Die Liste der Use-Cases lässt sich noch problemlos erweitern. Sie zeigt jedoch, dass es zwei Hauptprobleme gibt: die Sicherheit und der flexible Zugang für unterschiedlichste Bedürfnisse.

Verbote spiegeln Sicherheit vor

Das Thema Internet-Zugang in das eigene Intranet ist für viele Netzwerkadministratoren ein rotes Tuch, dem sie einfach per generellem Verbot einen Riegel schieben wollen und somit die Sicherheitsproblematik zu lösen glauben. Tatsächlich geschieht aber in den meisten Betrieben genau das Gegenteil. Da die Menschen, die dort arbeiten, reale Probleme zu lösen haben, finden sie auch Wege, um sich per moderner Telekommunikation Hilfe von außen zu verschaffen oder selber von außen Zugriff zu bekommen: Es werden Modems über Festnetz oder GSM Zugänge installiert, die außerhalb jeglicher Kontrolle stehen. Über diese Modems werden

dann von den verschiedensten Leuten diverse Software-Tools installiert, die eine Weile rege gebraucht werden und dann mit der Zeit in Vergessenheit geraten. Die Arbeit ist zwar erledigt, allerdings bleiben die Geräte noch in Betrieb, da vielleicht nochmals Support gebraucht wird. Die Sicherheitslöcher, die durch solche ‚Bastlerlösungen' entstehen, sind äußerst ernst zu nehmen. Das Bedürfnis nach Vernetzung einfach zu ignorieren, ist der falsche Weg. Entsprechende Verbote sind wirkungslos. Es ist daher unerlässlich, den Menschen die richtigen Werkzeuge in die Hand zu geben. Das heißt, einen Internetzugang anzubieten, der einerseits die verschiedenen Bedürfnisse tatsächlich abdecken kann, andererseits aber auch einen hohen Sicherheitsstandard aufweist. Letzteres bedeutet, dass die Architektur einerseits aus ihrer Konzeption heraus sehr robust gegenüber Attacken sein muss, andererseits soll sie sich auch durch eine gute Überwachbarkeit auszeichnen, so dass der Sicherheitsverantwortliche jederzeit weiß, wer was tut und ob das Sicherheitsdispositiv noch funktioniert.

Organisationsstruktur des Unternehmens abbilden

Das Internet-Gateway muss in der Lage sein, die verschiedensten Bedürfnisse abzudecken. Innerhalb des Intranets gibt es eine Vielzahl von Geräten und Systemen, die an einen Webserver angeschlossen sind oder selber über einen Embedded-Webserver verfügen. Diese Geräte werden für die unterschiedlichsten Zwecke eingesetzt, sind von verschiedenen Herstellern und unterscheiden sich in Bedienung und Funktionalität. Folglich muss der Netzwerkadministrator durch das Internet-Gateway in die Lage versetzt werden, den unterschiedlichsten Benutzergruppen spezifische Geräte zugänglich zu machen. Ferner muss es möglich sein, Privilegien für Lesen, Schreiben und Modifizieren gezielt an gewisse Personen zu vergeben. Außerdem sollte jede von extern durchgeführte Manipulation in einem Logfile abgelegt werden, zusammen mit der Information, wer den Eingriff ausführte.

Das Gateway sollte eine selektive Vermittlungsaufgabe wahrnehmen und auf keinen Fall spezifische Informationen über die Eigenschaften (wie MMI, Datenpunkte, Funktionen, etc.) eines angeschlossenen Gerätes speichern. Denn dadurch wird redundante Information geschaffen. Viele heute bekannte Konzepte verlangen den Anschluss jedes einzelnen Gerätes an ein übergeordnetes Leitsystem mittels eines speziellen Treibers. Es wird die Unterstützung eines spezifischen Interfaces verlangt, und durch die Installation eines Treibers wird redundante Information geschaffen. In einem verteilten System ist die Schaffung von redundanter Information schnell ein großes Problem, wie das folgende Beispiel zeigt.

Eine Firma liefert eine Maschine in eine Fabrik. Diese Maschine ist Teil einer komplexeren Produktionsanlage und muss nun in das Automations- und Steuerungskonzept integriert werden. Darin sind nun verschiedene Gruppen von Ingenieuren involviert. Die Maschine soll exakt kalibriert werden und hat gewisse Interaktionen mit benachbarten Systemen. Dazu wird der darauf integrierte Embedded-Webserver an das Gateway angeschlossen, und die Lieferfirma bekommt ein Login mit den Privilegien für den Zugriff auf ihre eigene Maschine. Bei der Kalibration zeigen sich verschiedene Probleme, und die Lieferfirma nimmt Modifikationen an der Firmware vor. Die Integration in die benachbarten Systeme zeigt auf, dass eine andere Interfacekommunikation notwendig wird und daher die Software und die Hardware nochmals modifiziert werden.

Bei einer richtigen Gateway-Architektur muss der Netzwerkadministrator ein neues Gerät (Embedded-Webserver) in sein Netzwerk integrieren sowie ein neues Login für einen externen Dienstleister definieren. Dies ist die typische Tätigkeit eines Netzwerkadministrators, und somit lässt sich der ganze Prozess der Fernwartung gut in eine Unternehmens-Organisationsstruktur integrieren.

Bei einer redundanten Gateway-Architektur muss bei jeder der beschriebenen Änderungen die entsprechende Anpassung auch auf dem Server nachvollzogen werden. Dies bedingt jedesmal, dass eine zusätzliche Person, die von der betreffenden Maschine nichts versteht, miteinbezogen werden muss. Denn die externe Firma darf den zentralen Gateway-Server sicher nicht auf eigene Faust administrieren. Zudem handelt man sich bei dieser Architektur die gefürchtete Versionsproblematik ein (ist die Treiberversion kompatibel mit dem Gerät?). Wichtig ist zusätzlich, dass die Lieferfirma den spezifischen Gateway-Standard überhaupt unterstützt. Dies ist nur ein Beispiel von vielen, das klar zeigt, dass der Aufbau von ‚Standard Gateway Interfaces' nicht nur unnötig, sondern in der Praxis katastrophal ist. Der notwendige Standard besteht nämlich bereits und wird allgemein unterstützt und eingehalten.

HTTP als einheitliches Vernetzungsprotokoll

Ein Gateway muss in der Lage sein, das http-Protokoll selektiv auf verschiedene Embedded-Webserver von Drittherstellern zu verteilen. Welche Funktionalität auf diesem Webserver verfügbar ist, ist Aufgabe des Lieferanten. Dieser ist die verantwortliche Instanz für das Funktionieren des Gerätes. Basierend auf dieser Erkenntnis lässt sich nun auch ein Sicherheitskonzept beschreiben, welches die geforderten Sicherheitsanforderungen erfüllt oder übertrifft.

Das Hauptproblem mit der Sicherheit besteht darin, dass das TCP/IP Protokoll im Normalfall mehr oder weniger transparent vom Internet bis ins Intranet verbunden wird. Durch die enorme Größe dieses Protokolls einerseits sowie der Komplexität der dabei involvierten Systeme andererseits entstehen dabei immer wieder Sicherheitslecks, die von Hackern ausgenutzt werden können. Durch ein Konzept, das ausschließlich auf das http-Protokoll aufsetzt, kann der Übertragungsweg ins Intranet wesentlich besser kontrolliert werden, indem das ‚reine http' auf einem Relais-Knoten vom TCP/IP getrennt wird und im Intranet in einem anderen Kontext wieder auf das Netz gebracht wird. Der wesentliche Unterschied zu einem Proxy-Server besteht darin, dass die Verbindung zum Internet nicht auf Protokollebene realisiert wird, sondern eher auf Applikationsebene. Der ganze TCP/IP Stack bietet somit für Attacken keine Angriffsfläche mehr.

Virtual Private Infrastructure

Ein wichtiger Aspekt ist, dass Sicherheit nicht nur theoretisch von der Technologie geboten werden kann, sondern auch dass der Aufwand dafür ‚im Felde' nicht zu groß ist. Hinzu kommt, wie robust sich das Konzept gegenüber Fehlbedienung oder unzureichendem Know-how der Verantwortlichen verhält. Gerade unter diesen Aspekten kann das http-Relais-Konzept seine Stärken voll ausspielen.

- Es entspricht dem Virtual Private Network (VPN) Konzept, aber auf Basis von Geräten anstatt von gesamten Netzwerken
- Das HTTP-Relais anstatt Proxyserver bringt die Sicherheit
- Es ist robust gegenüber Fehlbedienung
- Es gibt kein Routing des TCP/IP Protokolls ins Intranet
- Der Kunde initiiert die Verbindung und hat jederzeit die volle Kontrolle.

Beitrag als PDF im Internet