iniNet AG, Kompetenz in Informatik und Vernetzung
Seewenweg 5, CH-4153 Reinach, Tel. 061 716 96 26 Fax 061 716 96 17

SpiderControl™

Virtual Private Infrastructure für die Fernwartung per Internet

Das Thema ‚Embedded Internet' ist im Moment ein absolutes Modethema. Kaum eine Firma hat heute nicht irgend ein Produkt im Sortiment, dass 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 an den meisten Orten 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.
Wir möchten anhand eines realen Beispieles aus der Wirtschaft die auftretenden Probleme exemplarisch aufarbeiten und dabei aufzeigen, wie wichtig ein ganzheitlicher Ansatz und eine konsequente Architektur bei diesem Thema sind.

Beispiel aus der Praxis

Branche:
Service Automation

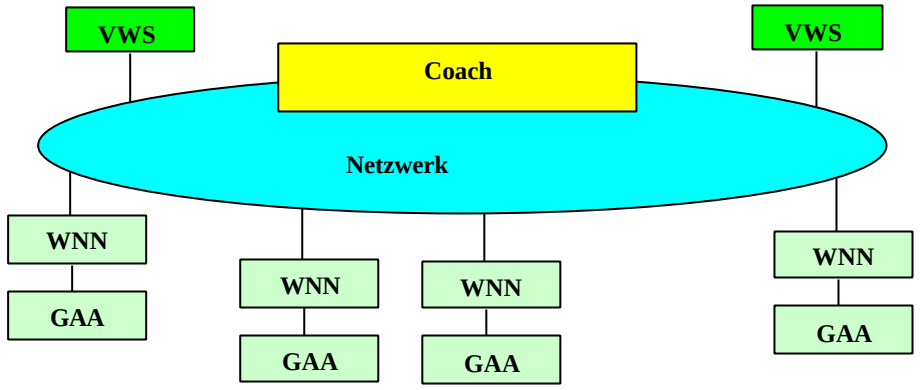
Bild 1: Bancomat

Projekt:
Webserverbasiertes Fernwartungs- und Diagnosesystem für Geldausgabeautomaten

Aufgabenstellung:
Der Kunde ist ein führender Anbieter im Bereich von Cash-Systemen. Die gewünschte Lösung sollte den Service für Bancomaten mit einer Web-Lösung ermöglichen. Ausserdem musste das Softwarekonzept in das bestehende Intranet eingebettet werden. Folgende Anforderungen wurden gestellt: Die Fernwartung aller Bancomaten sollte über einen Webserver erfolgen. Zusätzlich waren die Visualisierung der Tastatur, des Bildschirmes, des online-Journals und eine Alarmmeldung jedes einzelnen Bancomaten eine Voraussetzung. Geräteausfälle müssen mit der Aufgabenlösung erkannt und gezielt behoben werden können. Hervorzuheben bei dieser Lösung ist insbesondere der Umstand, dass der Service vieler Bancomaten nicht von der Bank selbst erledigt, sondern an eine Drittfirma untervergeben wird (Outsourcing). Da die Geldausgabeautomaten an das Intranet der Bank angebunden sind, ist die Sicherheitsfrage ein zentrales Thema, da diese Drittfirma von aussen über das Intranet der Bank Zugriff auf die Bancomaten erhalten muss.

Ziel:
Das Ziel war eine signifikante Reduktion des Serviceaufwandes. Bis anhin mussten alle Änderungen manuell vorgenommen werden.

Lösungsansatz:
Jeder Bancomat wird mit einem Embedded Webserver ausgerüstet. Weil über das Internet nicht direkt Zugriff auf die Bancomaten genommen werden darf, wurde basierend auf der SpiderControl™ Produktefamillie für embedded Web-Lösungen ein Zusatzgerät mit einer Microlinux-Applikation entwickelt. In diesem Gerät befinden sich jetzt alle Bedienseiten für die spezifische Automatenverwaltung. Mit dem zentralen Rechner werden periodisch oder auf Anfragen Alarmmeldungen gesichtet, aufbereitet und teilweise sogar online behoben. Ist z.B. der Bancomat leer? Ist das Journalpapier aufgebraucht? Sind zuviele Karten eingezogen worden? Welche Karten sind eingezogen worden etc.?



GAA: Geldausgabeautomat **WNN: Web Control Node**

Bild 2: Schematischer Ueberblick des Servicenetzwerkes

Ein interner oder externer Benutzer (VWS) erhält Zugang auf den zentralen Webserver (Coach), der als Gateway ausgelegt ist. Von dort aus kann er sich auf die einzelnen Bancomaten verbinden lassen.

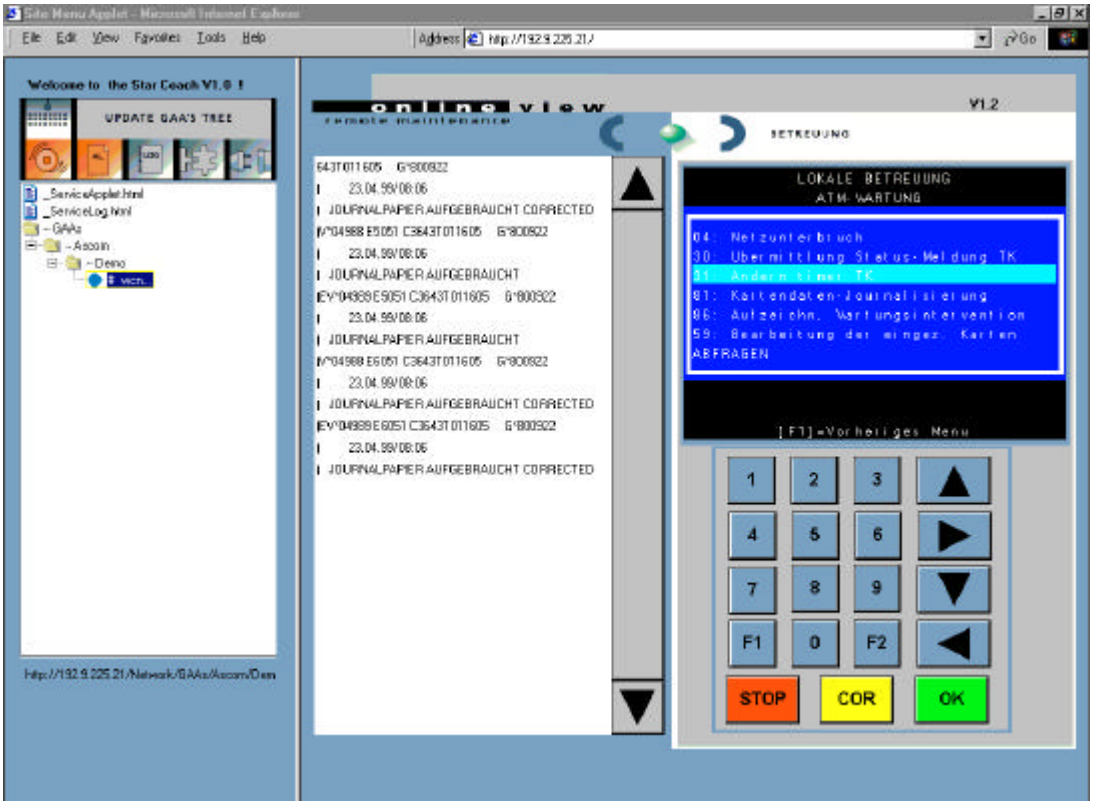


Bild 3: Bedieneroberfläche (Java Applet)

Wir sehen auf der linken Seite von Bild 3 eine Uebersicht aller angeschlossenen Geräte. Wird eine Störung erkannt, so wird der entsprechende Ast der

Baumdarstellung entsprechend gekennzeichnet. Auf der rechten Seite sehen wir die Bedieneroberfläche, auf die direkt vom embedded Webserver beim Bancomaten zugegriffen wird. Da eine Vielzahl von verschiedenen, teils auch älteren Bancomaten eingebunden werden muss, ist es sehr wichtig, dass das jeweilige Gerät seine eigene Oberfläche mitbringt. Der Coach muss somit lediglich die Adresse eines Bancomaten kennen, ein Update auf dem Coach beim Anschluss neuer Gerätetypen oder bei Modifikationen auf dem WNN entfällt.

Vorteile des Lösungsansatzes:

- Bis anhin wurden sämtliche Fehler vor Ort behoben. Dank dem Einsatz von Internet- und Intranettechnologie ist dies heute nicht mehr notwendig. Eine Vielzahl der Fehler kann von der „Zentrale“ aus behoben werden.
- Das neue System bietet Sicherheit. Durch die gewählte Architektur kann sichergestellt werden, dass ein externer Benutzer keinen Zugriff auf das Intranet erhält, sich aber trotzdem im Rahmen der im Coach definierten Netzwerkstruktur transparent und frei bewegen kann. Der Bancomat ist seriell an das WNN (Zusatzgerät) und das WNN per Intranet an den zentralen Computer angeschlossen.
- Die Ursache für Alarmmeldungen kann sofort erfasst werden. Durch die Embedded Webserver und die Verwendung des Daten-Webservers erhält der Benutzer Serviceinterfaces, welche den Zugriff auf einzelne Serviceseiten gestatten, mit welchem die Software- und teilweise auch Hardwarefunktionen überwacht und gesteuert werden können.
- Die grafischen Oberflächen gestalten die Benutzung äusserst einfach und bequem.

Im folgenden Kapitel möchten wir nun anhand des obigen Beispieles verallgemeinernd herausarbeiten, wo die Vorteile, aber auch Probleme liegen und wo vielfach Fehler gemacht werden können.

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. Das ist aber eigentlich nicht der Punkt. Der wichtigste Vorteil besteht nach unserer Erfahrung darin, dass man mit einem guten Gesamtkonzept mit Hilfe von Webtechnologien sehr viel Geld sparen kann. Wir unterscheiden zwei verschiedene Gebiete, in denen die Einsparungen erzielt werden können:

- Einsparungen bei der Software-Entwicklung
- Einsparungen durch veränderte Service- und Unterhaltskonzepte, die vorher nicht möglich (oder astronomisch teuer) waren

Die Ursachen für dieses Einsparungspotenzial sind vielfältig und bei jedem Projekt wieder etwas anders gelagert. Wir versuchen im Folgenden stichwortartig die wichtigsten Punkte zu nennen:

- Webtechnologie kann auf bereits bestehenden Ressourcen (Netzwerke) aufsetzen
- Vereinigt die Standards von Büroinformatik und Automation
- Flexiblere Lösungen
- Skalierbarkeit

Gesicherte Investition

- Bessere Wartbarkeit
- Plattformunabhängigkeit
- Grössere Zukunftssicherheit

Vermeidung von Investitionsruinen

Der Schlüssel zur Erschliessung des enormen Potenziales dieser Technologien liegt in einem guten Gesamtkonzept. Bestehende Lösungsmuster und Prozesse müssen umgedacht werden. Die Risiken, dass bei einer unkoordinierten Einführung einer neuen Technologie Investitionsruinen entstehen können, sind vorhanden. Wir möchten nun versuchen, auch die in anderen Projekten gemachten Erfahrungen einzubringen und 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 umsomehr 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 dann hernach noch vernetzt werden, sondern dass von Anfang an ein Gesamtsystem definiert werden muss, welches danach 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.
Der häufigste Fehler besteht darin, dass an irgendeinem Ort einmal begonnen wird, Web- Technologie einzuführen. Bevor es den meisten Beteiligten klar wird, werden dadurch Fakten geschaffen, die die Gesamtarchitektur des Konzeptes langfristig definieren, und meistens ist eine solcherart entstandene Architektur eine schwere Last. Bei verteilten Systemen werden konzeptuelle Fehler sehr viel schneller zum Verhängnis, weil die dezentralen Prozesse sehr schnell chaotischen Charakter annehmen können.
Es ist darum absolut unerlässlich, von Anfang an ein wirklich gutes und stabiles Konzept zu definieren. Das heisst, es sollten von Anfang an alle möglichen Anforderungen in das Konzept mit einfliessen.
Dies heisst insbesondere, dass alle möglichen ‚Use-Cases' von Anfang an berücksichtigt werden. Es hat sich als ratsam erwiesen, auch diese Anwendungsfälle mit in die Planung einzubeziehen, welche im Moment gar nicht vorgesehen sind. Dies lässt einerseits für die Zukunft alle Optionen offen, macht aber andererseits das Design in der Zukunft flexibler gegenüber neuen Anforderungen, welche man sich im

Moment noch gar nicht vorstellen kann. Kurz gesagt heisst das, man unterstützt heute Anforderungen, die man kennt, aber nicht braucht, um in Zukunft leichter Bedürfnissen entsprechen zu können, die man heute noch nicht kennt. In einem vernetzten Umfeld macht dies das Design nicht komplexer, sondern besser. Entsprechende Erweiterungen auf der einzelnen Hardware müssen ja nicht ausprogrammiert, sondern nur konzeptuell vorgesehen werden.

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 physische Verbindung ist zwar ein wichtiger Aspekt (v.a. in Bezug auf Sicherheit), die wesentliche Frage stellt sich jedoch darin, welche Dienste wie angebunden werden, für wen diese zugänglich sind, was man damit machen kann, wie diese verwaltet werden und wie sie in Zukunft erweiterbar sind.
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

Wenn wir uns nun überlegen, welche Tätigkeiten diese Personen ausführen könnten und welche Geräte und Maschinen dafür in Frage kommen, so 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. Gewisse dieser Konzepte werden bereits fertig mit dem Gerät ausgeliefert und können nicht geändert werden, andere Webanbindungen werden vom Systemintegrator selber gemacht. Wir haben nun die Aufgabe, alle diese Systeme derart mit dem Internet zu verbinden, dass die verschiedenen Benutzergruppen selektiv auf ‚ihre' Systeme zugreifen können.

Die Liste der Use-Cases lässt sich noch problemlos erweitern. Sie zeigt uns jedoch auch schon so, dass wir zwei Hauptprobleme lösen müssen:

- Sicherheit
- Flexibler Zugang für unterschiedlichste Bedürfnisse

‚Verbote spiegeln vermeintliche 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 still und heimlich 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 sich ausserhalb jeglicher Kontrolle befinden. Ueber 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, weil die Arbeit soweit erledigt ist, die Geräte aber noch in Betrieb bleiben, weil ja vielleicht nochmals Support gebraucht wird. Die Sicherheitslöcher, die durch diese Bastlerlösungen entstehen, sind äusserst ernst zu nehmen, und es ist eine Illusion, zu glauben, dass man das Bedürfnis nach Vernetzung einfach ignorieren und ein Verbot auch eingehalten werden kann. 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 ggenüber Attacken sein muss, andererseits soll sie sich auch durch eine gute Ueberwachbarkeit auszeichnen, sodass der Sicherheitsverantwortliche jederzeit weiss, wer was tut und ob das Sicherheitsdispositiv noch funktioniert.

‚Das Internet-Gateway muss in der Lage sein, die Organisationsstruktur des Unternehmens abzubilden'

Wie wir gesehen haben, muss das Internet Gateway in der Lage sein, die verschiedensten Bedürfnisse abzudecken. Wir können davon ausgehen, dass innerhalb des Intranets eine Vielzahl von Geräten und Systemen vorhanden sind, die an einen Webserver angeschlossen sind oder selber über einen emedded 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.
Es zeigt sich deutlich, dass das Gateway eine selektive Vermittlungsaufgabe wahrnehmen muss und auf keinen Fall spezifische Informationen über die Eigenschaften (wie MMI, Datenpunkte, Funktionen, etc.) eines angeschlossenen Gerätes speichern sollte, weil dadurch redundante Information geschaffen wird. Viele heute bekannte Konzepte verlangen den Anschluss jedes einzelnen Gerätes an ein übergeordnetetes 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 sehr schnell ein riesiges Problem, wie wir mit dem folgenden Beispiel verdeutlichen möchten:
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. Nehmen wir nun an, die Maschine muss 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 nun verschiedene Probleme, und die Lieferfirma macht verschiedene Modifikationen an der Firmware. Die Integration in die benachbarten Systeme zeigt nun auf, dass eine andere Interfacekommunikation notwendig wird und daher SW und HW 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 nun bei jeder der beschriebenen Aenderungen 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 ?). Die erste Bedingung ist zusätzlich, dass die Lieferfirma den spezifischen Gateway Standard überhaupt unterstützt. Dies ist nur ein Beispiel von vielen, welches aber schon klar zeigt, dass der Aufbau von ‚Standard Gateway Interfaces' nicht nur unnötig, sondern in der Praxis katastrophal ist. Der notwendige Standard besteht nämlich schon und wird allgemein unterstützt und eingehalten.

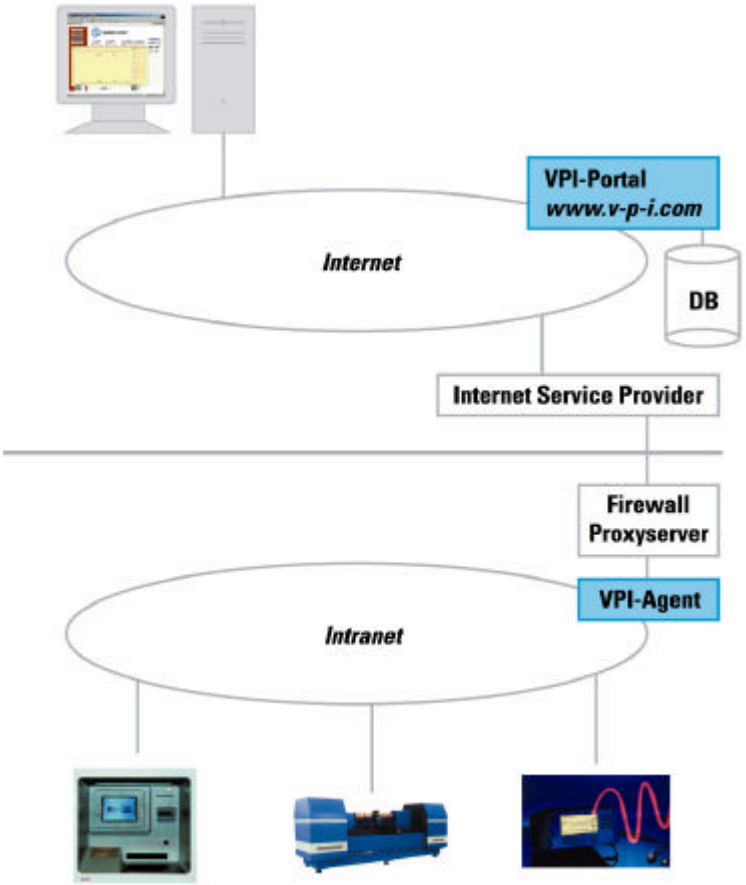
‚Das einheitliche Vernetzungsprotokoll existiert bereits: HTTP'

Wir sehen, dass ein Gateway in der Lage sein muss, dass http-Protokoll selektiv auf verschiedene embedded Webserver von Drittherstellern zu verteilen. Welche Funktionalität auf diesem Webserver verfügbar ist, ist Aufgabe des Lieferanten. Dieser ist schliesslich 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 Mächtigkeit dieses Protokolls einerseits sowie der Komplexität der dabei involvierten Systeme andererseits entstehen dabei immer wieder Sicherheitslecks, die von Hackern ausgenutzt werden können. Da wir ein Konzept verfolgen, welches ausschliesslich auf das http-Protokoll aufsetzt, kann dadurch der Uebertragungsweg ins Intranet wesentlich besser kotrolliert werden, indem das ‚reine http' auf einem Relais-Knoten vom TCP/IP getrennt wird, um 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: Sicherheit + Einfachste Anbindung ans Internet'

Ein ganz wichtiger Sicherheitsaspekt ist auch darin zu sehen, dass es nicht nur darum geht, ob die Sicherheit von der Technologie her theoretisch geboten werden kann, sondern auch, ob der Aufwand dafür ‚im Felde' nicht zu gross ist, und schliesslich, wie robust sich das Konzept gegenüber Fehlbedienung oder eben unzureichendem Know-How der Verantwortlichen verhält. Gerade unter diesen Aspekten kann das http-Relais Konzept seine Stärken voll ausspielen.

- Entspricht dem Virtual Private Network (VPN) Konzept, aber auf Basis von Geräten anstatt von gesamten Netzwerken
- HTTP-Relais anstatt Proxyserver bringen die Sicherheit
- Robust gegenüber Fehlbedienung
- Kein Routing des TCP/IP Protokolls ins Intranet
- Der Kunde initiiert die Verbindung und hat jederzeit die volle Kontrolle



Typische Fehler

Wir möchten im Folgenden einige typische Erwartungen aufzeigen, die ein falsches Bild der Problematik wiederspiegeln.

Fehler 1: ‚Mit der Integration eines embedded Webservers ist das Problem gelöst. Für den Rest gibt es Standard-Internet Tools'
Embedded Webserver sind erst 10% der Lösung, die wahren Probleme beginnen damit erst. Standard Internet Tools verwenden zwar die gleiche Basistechnologie, sind aber für ein völlig anderes Einsatzprofil konzipiert. Tatsächlich entfernen sich die Technologien je länger je mehr, sodass beispielsweise die Gestaltung von Bedieneroberflächen mit Standard-Tools auf einem embedded Webserver die dort vorhandenen Ressourcen komplett überfordert (Stichwort: Thin Client - Fat Server). Die Beherrschung der richtigen Technologie für die MMI's ist aber meistens noch gar nicht das Hauptproblem. Es ist wichtig, die gestellte Aufgabe als gesamtheitliches Konzept zu lösen. Dies bedeutet, das gesamte Netzwerk, auf dem das System eingesetzt wird, als System zu betrachten, und an den richtigen Stellen die richtigen Komponenten einzusetzen. Der Aufbau von Insellösungen führt sehr schnell in eine Sackgasse. Auch für einen Hersteller von embedded Komponenten ist es zentral wichtig, welchen Nutzen er mit einem embedded Webserver für seine Kunden erzielen kann. Der Nutzen entsteht aber erst mit der richtigen Netzwerkintegration. Das Netzwerk ist die Applikation, nicht der Microcontroller.

Fehler 2: ‚Fernwartung per Modem ist am einfachsten und sichersten.'
Die Punkt-zu-Punkt Verbindung per Modem ist zwar am schnellsten zu realisieren, bringt aber die bereits beschriebenen Sicherheitsprobleme mit sich. Ab einer bestimmten Grösse eines Unternehmens wird es absolut unkontrollierbar, wer wo welche Eingriffe vornimmt. Fernwartung sollte sich in die bestehenden Organisationsstrukturen der Firma einbinden und die bestehenden Netzwerke verwenden.

Fehler 3: ‚Netzwerke sind transparent.'
Intranets sind vielfach über Router und Switches verbunden und in Unternetzwerke segmentiert. Für die PC-Benutzer innerhalb einer Firma werden entsprechende Netzwerkkonfigurationen vorgenommen, um die Transparenz soweit wie nötig zu gewährleisten. Transparente Netzwerke für die PC's einer Firma und für den Zugriff eines externen Internet-Clients sind technisch zwei verschiedene Dinge und es ist für die Sicherheit unerlässlich, dass diese Anforderungen auch logisch getrennt gelöst werden. Auf Basis des http-Relais Konzeptes ist dies sehr gut realisierbar.

Fehler 4: ‚Fernwartung ist ein Add-On zum bestehenden Betriebsleitsystem.'
Die Anforderungen an den Fernzugriff per Internet sind weit grösser, weil dieser für verschiedenste Benutzergruppen offen sein muss. Um das Einsparungspotenzial der Technologie zu erschliessen, ist es unerlässlich, dass gerade dieses ‚zentralistische' Konzept eines Betriebsleitsystemes nicht weitergeführt wird.

Die Firma iniNet AG ist spezialisiert auf Internettechnologien im industriellen Umfeld und hat für diesen Bereich die ‚SpiderControl ä ' Produktefamillie entwickelt.
Zusammen mit unseren Partnerfirmen können wir europaweit Lösungen entwickeln und beraten.

iniNet AG
Seewenweg 5
CH-4153 Reinach
Switzerland