Sichere Datenverbindungen für Infrastrukturanwendungen

Inhärent sichere Konzepte als Alternative zu IP-SEC und VPN

Solange Fernwartung über IP-Verbindungen auf Firmen- und Werksgelände beschränkt war, konnten Hacker sich nur schwer Zugang zu den empfindlichen Anlagen verschaffen. Doch seit Fernwartung im Zeitalter des „Internet of Things" auch über öffentliche Netze (Internet, GPRS, UMTS) erfolgt, mehren sich die Berichte über unerlaubte Zugriffe. Gut wenn es nur „white Hacker" sind, die auf ungeschützte Passwortlisten oder Zugriffsmöglichkeit über offene Internetports aufmerksam machen wollen. Auch Spaßvögel haben schon mit Hilfe von Fernschaltfunktionen um Mitternacht die Kirchenglocken läuten lassen und das Licht im Klärwerksgebäude eingeschaltet. Hier helfen die in der IT üblichen Techniken mit Nutzung komplexer Passworte, Anwendung von SSL bzw. TLS und der Einsatz von IP-Sec und VPN. Doch diese Maßnahmen sind komplex in der Durchführung und aufwendig angesichts der Vielzahl der Systeme im Feld (Front-End), die in die Sicherheitsarchitektur einbezogen werden müssen. Systemadministratoren stöhnen mittlerweile über das Einrichten der vielen VPN-Tunnel, das Aktualisieren der Router und Front-Ends mit Sicherheits-Patches und anderen Updates. Und so steht man vor der Wahl: Entweder man steckt viel Geld und Zeit in die Systempflege oder man wird zum potentiellen Angriffsziel. Es scheint nur eine Frage der Zeit, bis kriminelle Hacker ein Stadtwerk bedrohen oder andere Ziele ausmachen. Glaubt man Spekulationen, so gab es bereits Vorfälle, die mit Zahlung eines Lösegelds abgewendet wurden. Dieses Dilemma zwischen hohem Aufwand oder potenzieller Unsicherheit kann man auflösen, indem man die Front-End- Systeme aus der Welt der sicherheitskritischen Systeme gänzlich herauslöst und alle für Angriffe relevanten Prozesse auf den einen Zentralrechner in der Leitwarte – auch Back-End genannt – konzentriert. Dann muss an Stelle vieler kleiner Systeme im Feld nur noch diese eine zentrale Datenbank nach den Regeln der IT- Sicherheit geschützt werden und der Aufwand wird deutlich verringert.

Analyse der Sicherheit von Fernwirk- und Fernwartungstechnik

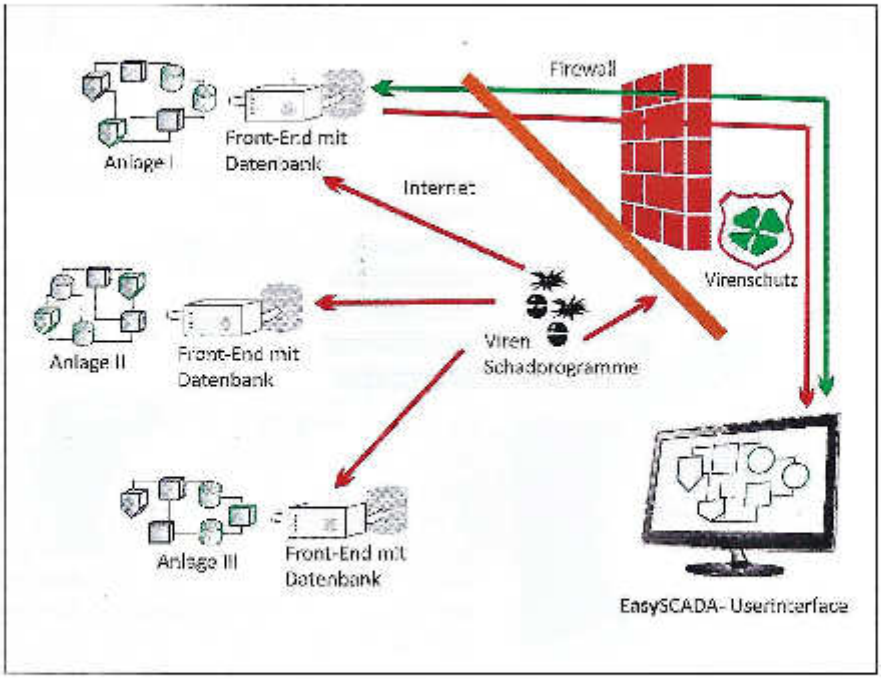
Bei der wireless netcontrol GmbH wurde das Thema der Sicherheit von Fernwirk- und Fernwartungstechnik von Grund auf analysiert und die bekannten zwar leistungsfähigen aber leider auch angreifbaren Techniken auf den Prüfstand gestellt.

Folgende Aspekte konnten herausgearbeitet werden:

- Die Ansprüche an moderne Fernwartung sind gestiegen. Der Anwender fordert grafische Oberflächen und will jederzeit auf große Datenbestände zugreifen, zum Beispiel um Zeitverläufe darzustellen oder statistische Auswertungen zu erstellen. Die dafür erforderlichen Daten und Nutzeroberflächen sollten aber zweckmäßiger Weise zentral gespeichert, gesichert und geschützt werden.
- Die Front-End-Systeme beinhalten leistungsfähige Kleinrechner, sehr oft auf LINUX-Basis, die nur mit sehr viel Fachwissen und Aufwand sicher gemacht werden können. Für automatisierte Softwarewartung geöffnete Ports sollen diese Arbeiten automatisieren, bilden aber selbst ein hohes Sicherheitsrisiko für den Eintritt von Schadsoftware, die sich als Firmware-Update tarnt.
- Die Front-End-Systeme benötigen einen Großteil der Parametrier- und Einstellfunktionen gar nicht, bzw. diese werden praktisch nie genutzt. Es ist eigentlich gar nicht nötig, für einfache Aufgaben wie die Erfassung verschiedener Temperaturmesswerte über das Internet auf einen Kleinrechner mit (unsicherem) Betriebssystem, 32 GB Datenspeicher, Browser, E-Mailprogramm zuzugreifen. Die gleiche Funktionalität kann man einfacher und sicherer realisieren, damit Schadsoftware keine Plattform geboten wird, auf der sie wirksam agieren kann.
- Die Leistungsfähigkeit der in den Front-End-Systemen verbauten Kleinrechner und die gewachsenen Möglichkeiten des Internets verführt zu einem hohen, eigentlich völlig sinnlosen Datentraffic, indem über das Internet auf die lokalen Bedienoberflächen des Front-End zugegriffen wird. Um regelmäßig einen Satz von 10 Temperaturmesswerten abzurufen würde es reichen, genau diese Werte vom Front-End zum Back-End zu transportieren. In der Realität werden aber ganze grafische Bedienoberflächen auf dem Front-End aufgerufen und dann natürlich auch zum Back-End transferiert. Dies erfolgt in jedem Einzelfall wieder aufs Neue. Wären die Informationen von vornherein schon beim Back-End verfügbar, wäre damit sogar der Komfortzuwachs verbunden, dass das Benutzerinterface schneller zur Verfügung stünde.

Front-End-Geräte mit von außen nicht veränderbarer Software

Auf der Grundlage dieser Überlegungen wurde das EasySCADA-System konzipiert, das als Front-End mit dem Datentransmitter GO WirelessConnect arbeitet. Das für



Bei der automatisierten Softwarewartung stellen die dafür geöffneten Ports ein hohes Sicherheitsrisiko dar.

die Datensicherheit Bemerkenswerte ist, dass diese Front-End-Geräte über eine per Datenzugriff von außen nicht veränderbare Software verfügen, die dadurch für keinerlei Manipulation zugänglich ist. So findet Schadcode aus dem Internet keinen Ansatzpunkt (inhärent sicher) und Softwareupdates können ausschließlich lokal eingespielt werden.

GO WirelessConnect

Um allen Hardwareanforderungen der Fernwirktechnik gerecht werden zu können, besteht das GO WirelessConnect aus einem Zentralgerät, das um Funktionsbausteine erweitert werden kann. Angeboten werden GO Module für die Aufnahme von Messwerten, für Signale von Grenzwertgebern (schaltend) sowie Aktoren mit Schaltfunktion. Neben diesen Basisfunktionen sind Module für den M-BUS, den wireless M-BUS und die Impulszählung (auch für die S0-Schnittstelle) verfügbar. Durch diese Funktionsvielfalt kann sich der Anwender jederzeit flexibel an die Aufgabenstellung anpassen und deckt genau die Aufgaben ab, die er für sein Fernwartprojekt benötigt. Die Anlage ist durch weitere Funktionsmodule jederzeit erweiterbar oder kann um Module reduziert werden, wenn diese nicht mehr benötigt werden.

Das GO WirelessConnect agiert vorwiegend als Datensammler, so dass die anderen Aufgaben des Gesamtsystems, wie Speicherung und Weiterverarbeitung der Messwerte sowie deren Sicherung gegen Verlust und Schutz vor unberechtigtem Zugriff auf das Back-End verlegt werden. Dies ist entsprechend der gewählten Sicherheitsarchitektur auch sinnvoll, denn hier können alle Maßnahmen der IT-Sicherheit an einer zentralen Stelle ausgeführt und auf dem aktuellen Stand gehalten werden. Dies ist gerade bei großen Fernwartungsnetzen eine unschätzbar große Erleichterung, die sehr viel Zeit und Aufwand spart.

Zentrales Element ist eine SQL-Datenbank

Zentrales Element des Gesamtsystems ist eine SQL-Datenbank, in der die permanent von dem Front-End übertragenen Fernwartungsdaten in einem allgemein verwendbaren Standardformat gespeichert werden. In der Datenbank sind die Daten aller Front-End sowie die Anlagenhistorie langfristig sicher und auch nach Jahren und Jahrzehnten noch nutzbar.

Am Ende jedes SCADA-Systems steht die Prozessvisualisierung, die über entsprechende Auswahlmöglichkeiten die erfassten Daten für den Benutzer anschaulich zugänglich macht und Möglichkeiten zur Auswertung liefert. Sowohl der Ebenenaufbau als auch Umfang und Funktionalität einer Prozessvisualisierung können sehr unterschiedlich sein und hängen stark von den Anlagen oder Gebäuden ab, die an das Fernwartungssystem angegliedert sind. Auch die Gruppen von Nutzern und ihre Berechtigungen im System spielen eine Rolle und können sehr verschieden sein. Daher wird das SCADA nach den Anforderungen des Anwenders individuell gestaltet und für den spezifischen Fall eingerichtet.

EasySCADA

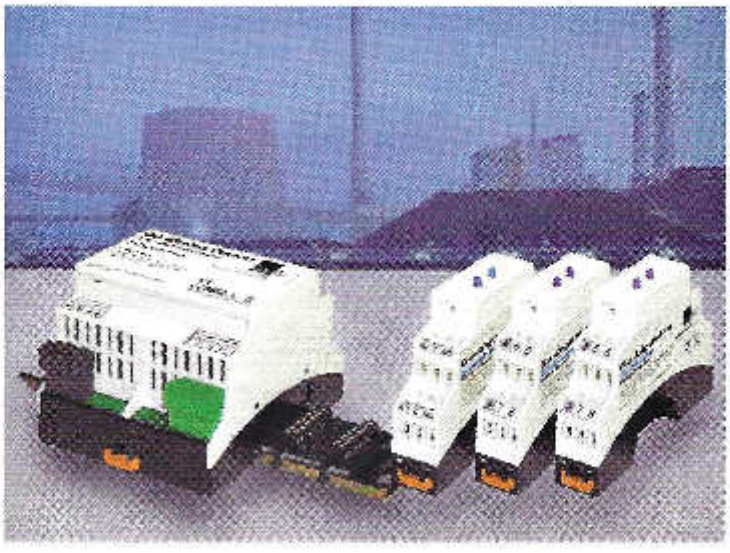
Obwohl GO WirelessConnect und die SQL-Datenbank für verschiedene SCADA-Visualisierungen offen sind, kann dieser sehr wichtige Teil des Gesamtsystems durch die im Leistungspaket enthaltene EasySCADA-Softwareumgebung schnell und professionell gelöst werden. Die Idee von EasySCADA besteht darin, die gesamte SCADA-Funktionalität, die mehrere Ebenen umfassen kann, auf einer durchsichtigen Ebene, dem so genannten „Transparent Layer" abzubilden. Die einzelnen Sensoren oder Aktoren können dort beliebig platziert und in dem Sinn der Anlage entsprechend angeordnet werden. Diese transparenten Ebenen werden in einem weiteren Schritt mit Abbildungen der zu steuernden Anlage unterlegt, so dass der Zusammenhang mit dem Aufbau der Anlage hergestellt wird. Die Anlagenbilder unter dem „Transparent Layer" können ganz unterschiedlicher Art sein. Verwendbar sind zum Beispiel die typischen technischen Darstellungen aber auch Luftaufnahmen oder Pläne aus der Phase der Anlagenprojektierung. Der wesentliche Vorteil von EasySCADA ist dabei ein ungewöhnlich gutes Nutzen zu Kosten-Verhältnis.

Fazit

Ob eines der bekannten SCADA-Softwarepakete gewählt wird oder EasySCADA zum Einsatz kommt: In jedem Fall erhält der Anwender mit GO WirelessConnect ein Fernwartungssystem, das sicher ist und den Zeitbedarf für die Systemadministration gering hält. Alle Sicherheitsfragen sind auf den zentralen Datenbankrechner beschränkt, der auch das Back-End für die Prozessvisualisierung bildet. Diese Systemarchitektur bildet das auch von der Kostenseite her betrachtet entscheidende Argument, sich für EasySCADA und GO WirelessConnect zu entscheiden.

Autor: Dr. Ulrich Pilz, Geschäftsführer bei Wireless Netcontrol

■ *WIRELESS NETCONTROL GmbH*
www.wireless-netcontrol.de



Das GO WirelessConnect besteht aus einem Zentralgerät, welches um Funktionsbausteine erweitert werden kann.