Inhärent sichere Konzepte

Alternative zu IP-SEC und VPN

BU

Bild: Wireless Netcontrol GmbH

Klassische Sicherheitsmaßnahmen für das industrielle Internet der Dinge sind komplex und aufwendig. Anwender und Betreiber stehen vor der Wahl: Entweder viel Geld und Zeit investieren oder eine hohe Unsicherheit in Kauf nehmen. Ein neues System setzt hier auf Front-End-Geräte, die über eine per Datenzugriff von außen nicht veränderbare Software verfügen. Damit sind sie für keinerlei Manipulation zugänglich.

Solange Fernwartung über IP-Verbindungen auf Firmen- und Werksgelände beschränkt war, konnten sich Hacker nur schwer Zugang zu den empfindlichen Anlagen verschaffen. Doch seit Fernwartung im Zeitalter des Internet der Dinge auch über öffentliche Netze 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. 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 Ansätze wie komplexe 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 dann schnell über das Einrichten der vielen VPN-Tunnel oder das updaten der Router und Front-Ends mit Sicherheits-Patches. Entweder man steckt also 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. 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. Beim Unternehmen Wireless Netcontrol wurde die Sicherheit von Fernwirk- und Fernwartungstechnik von Grund auf analysiert und die bekannten zwar leistungsfähigen aber leider auch angreifbaren

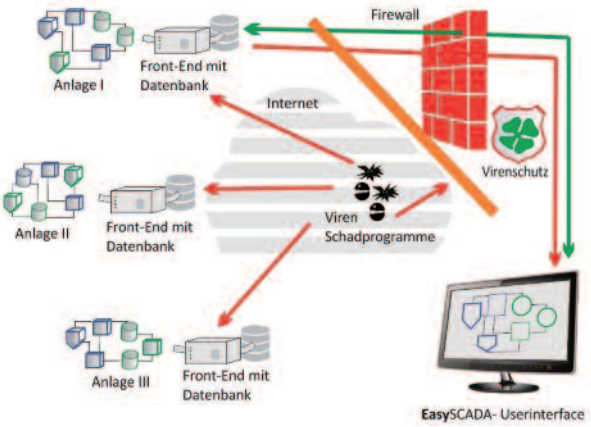

Bild: Wireless Netcontrol GmbH

BU

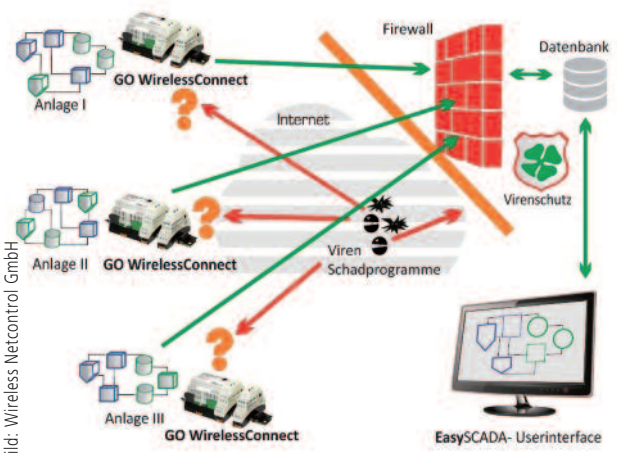

Bild: Wireless Netcontrol GmbH

BU

Ansätze auf den Prüfstand gestellt. Folgende Aspekte konnten herausgearbeitet werden:

- Die Ansprüche an moderne Fernwartungskonzepte sind gestiegen. Der Anwender fordert grafische Oberflächen und will jederzeit auf große Datenbestände zugreifen, z.B. um Zeitverläufe darzustellen oder statistische Auswertungen zu erstellen. Die dafür erforderlichen Daten und Nutzeroberflächen sollten aber zweckmäßiger Weise zentral gespeichert, gesichert und geschützt werden.
- Viele Front-End-Systeme beinhalten leistungsfähige Kleinrechner, die nur mit Fachwissen und großem Aufwand sicher gemacht werden können. Für automatisierte Software-Wartung geöffnete Ports sollen diese Arbeiten erleichtern, bilden aber selbst ein hohes Sicherheitsrisiko für den Eintritt von Schad-Software, die sich als Firmware-Update tarnt.
- Front-End-Systeme benötigen einen Großteil der Parametrier- und Einstellfunktionen gar nicht, bzw. werden diese 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, 32GB Datenspeicher, Browser und E-Mailprogramm zuzugreifen. Die gleiche Funktionalität kann man einfacher und sicherer realisieren, damit Schad-Software 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 Daten-Traffic, indem über das Internet auf die lokalen Bedienoberflächen des Front-End zugegriffen wird. Um regelmäßig einen Satz von zehn 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. Das 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.

Auf der Grundlage dieser Überlegungen wurde das EasyScada-System konzipiert, das als Front-End mit dem Datentransmitter GO WirelessConnect arbeitet. Das für 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 Software Updates können ausschließlich lokal eingespielt werden.

Zentralgerät und Funktionsbausteine

Um allen Hardwareanforderungen der Fernwirktechnik gerecht werden zu können, besteht das GO WirelessConnect aus einem Zentralgerät, das um Funktionsbausteine erweitert werden kann. Angeboten werden Module für die Aufnahme von Messwerten, für Signale von Grenzwertgebern (schaltend) sowie Aktoren mit Schaltfunktion. Neben diesen Basisfunktionen sind Module für M-Bus, wireless M-Bus und Impulszählung (auch für die S0-Schnittstelle) verfügbar. Durch diese Funktionsvielfalt kann sich der Anwender an die Aufgabenstellung anpassen und genau die Aufgaben abdecken, 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. 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. Das 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. Gerade bei großen Fernwartungsnetzen spart diese Erleichterung viel Zeit und Aufwand. 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.

Individuelle Scada-Gestaltung

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. 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 Software-Umgebung EasyScada schnell und professionell gelöst werden. Die Idee hinter dem Tools 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 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 gutes Kosten/Nutzen-Verhältnis. Ob eines der klassischen 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. ■

Autor: *Dr. Ulrich Pilz*
Geschäftsführer
Wireless Netcontrol GmbH
www.wireless-netcontrol.com

Direkt zur Marktübersicht *www.i-need.de/ 43*