Anlagen über Internet steuern

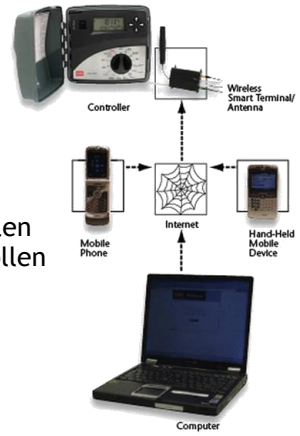
Neue schöne Welt – die Werbung verspricht's

„Eltern beenden heute die Party des jugendlichen Nachwuchses von unterwegs aus: Sie schalten das Licht aus, kühlen die Heizung herunter und legen statt wilder Party Musik per Smartphone Bachs Sonate in g-Moll im heimischen Wohnzimmer auf."

Immer mehr Hersteller setzen heute auf die moderne und bequeme Steuerung von Anlagen über das Netzwerk und das Internet. Bei unserer Arbeit für unsere Kunden begleiteten wir Steuerungen für

- Solar-Module und Einspeisungen von Öko-Strom ins öffentliche Stromnetz
- Anlagen für Heizung, Lüftung, Klimatisierung und Sonnenschutz
- Überwachungseinrichtungen, Videokameras, Alarmanlagen und Zutrittskontrollen
- Licht- und Sound-Steuerungen, Gebäudeautomatisierung und Kraftwerk-Kontrollen

Dabei sind die Steuerungsanlagen gar nicht neu. Neu ist vielmehr die elektronische Fernsteuerung über Netzwerke und neuerdings eben auch immer einfacher über das Internet und über Smartphones.



Original Werbe-Darstellung

Tag der offenen Tür: Aufgeklärt verstehen

Viele Hersteller erweitern ihre bisherigen System-Steuerungen um Netzwerk-Schnittstellen von Zuliefer-Unternehmen. Ziele sind dabei natürlich vor allem die einfache Bedienung und niedrige Kosten.

Und so sind Fernsteuerungen schnell und praktisch startklar – inkl. App auf dem Smartphone. Über die Sicherheit des Systems sagt dies nichts Gutes aus: Jeder, wirklich jeder, der das Kennwort kennt oder herausfindet hat Zugriff über Netzwerk und Internet.

Folgende Aspekte zeigen, wie einfach Kriminelle ganze Maschinenparks unter ihre Kontrolle bringen:

- Schützt Ihre Systemsteuerung vor falscher Kennworteingabe?
  Bei den meisten Anlagensteuerungen ist es nur eine Frage der Zeit, bis ein „Hacker" mit seinem Computer das Kennwort durch einfaches ausprobieren „erraten" hat. Für solche „*Brute Force*"-Angriffe braucht ein normaler PC zuhause bei einem 8-stelligen Passwort heute nur noch weniger als einen Monat.
- Verschlüsselt Ihre Anlagensteuerung die Passwortübertragung?
  In vielen Fällen ist der Einsatz von Verschlüsselung (z.B. mittels SSL über HTTPS) nicht vorgesehen oder unvollständig konfiguriert. Meist kommen Standard SSL-Schlüssel zum Einsatz, die auch dem Angreifer bekannt sind. Das vermeintlich sicher geglaubte Passwort kann so bei der Übertragung ausspioniert werden. Und die Anlage wurde ganz ohne Virus „gehackt".
- Wer liefert Software-Updates für ständig bekannt werdende Sicherheitslöcher?
  Sicherheitstechnik in Software (z.B. Verschlüsselung) muss ständig gepflegt werden. Die meisten Hersteller sind nicht in der Lage, für jede Schwachstelle zeitnah (z.B. monatlich) ein Update zu liefern, auch weil jedes Sicherheitsupdate zunächst in die eigene Anlagen-Software integriert werden muss. Oft werden dabei Fehler gemacht, die zu neuen Sicherheitslöchern führen.

Bis hin zur Gefahr für Leib und Leben

Mangelhaft geschützte Systeme sind eine Einladung zur Industriespionage, insbesondere im Bereich Forschung und Fertigung. Doch damit nicht genug: Über einen Fremd-Zugriff auf Server und Anlagen könnten diese abgeschaltet oder mit neuen Aufträgen versehen werden.

Die Folgen reichen vom Imageverlust und finanziellen Schäden über defekte Maschinen bis hin zu einer realen Gefährdung für Leib und Leben – stellen Sie sich den Ausfall einer Heizung in einem Altenheim vor oder unerwartete Anlagen-Kommandos während Wartungsarbeiten an Solarmodulen.

Hotline: (0800) 0 60 8000
service@all-connect.net | www.all-connect.net

all-connect Data Communications GmbH
Maistraße 12 | 80337 München | Tel: +49 (89) 55 296-0 | Fax: +49 (89) 55 296-499
HRB 122790, AG München | Geschäftsführer: Michael Henle | USt-ID: DE 197110167