Auszug aus dem Whitepaper „Web-Technologie in der Automation“

Wichtige Sicherheitsaspekte beim Einsatz von Saia PCD® Steuerungen und HMI im Internet/LAN.

Erstdruck: 2007

Sicherheit

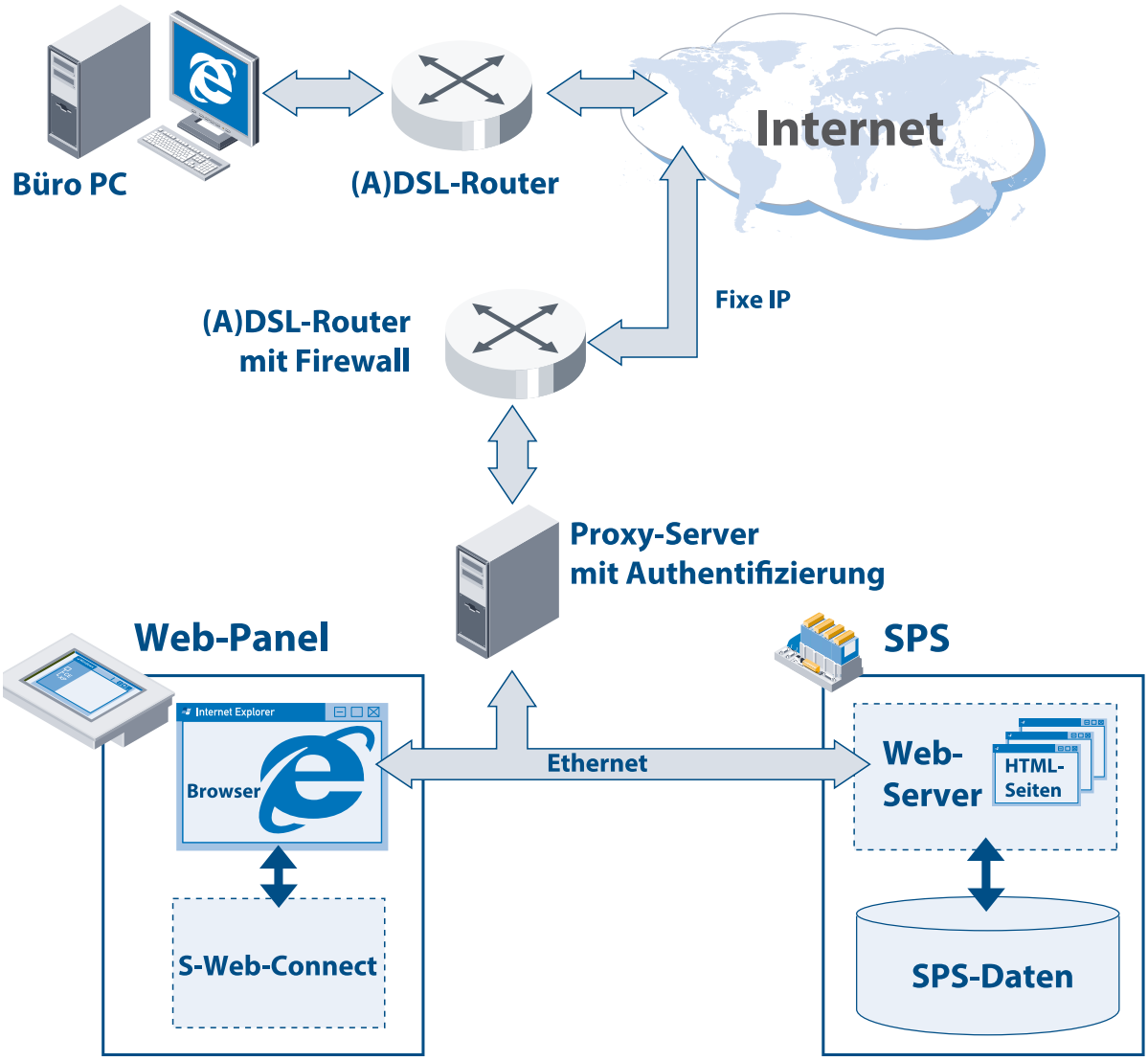
Wenn es um Web-Technik geht, kommen früher oder später Fragen zum Thema Sicherheit auf. Kaum vergeht ein Tag, an dem uns nicht weisgemacht worden soll, dass unser Windows®-PC angeblich nicht sicher ist. Mittlerweile lebt eine ganze Industrie von der Furcht vor Hacker- und Viren-Attacken. Das soll nicht heissen, dass das Thema Sicherheit nicht ernst zu nehmen ist, aber eine objektivere und nüchterne Betrachtung tut trotzdem Not.

Microsoft® hat tatsächlich ein Problem mit der Sicherheit: Man hat sich dem Thema unvorsichtigerweise angenommen. Nun ist ein Betriebssystem allerdings der denkbar schlechteste Ort, einen wirkungsvollen Schutz aufzubauen. Das liegt zum einen an der Komplexität heutiger Betriebssysteme. Andererseits überzeugt der Gedanke an einen wirksamen Schutz nicht, wenn der Eindringling bereits auf dem Rechner angekommen ist. Daher wird im professionellen Umfeld das Thema Sicherheit losgelöst von der einzelnen Arbeitsstation (also dem einzelnen PC) angegangen. Hierzu gibt es dedizierte Komponenten, welche die Schutzfunktion stand-alone erbringen, z.B. eine HW-Firewall. Meist beinhalten (A)DSL-Router ohnehin eine Firewall, welche in ihrer Wirksamkeit einer auf PCs installierten SW-Firewall allemal vorzuziehen ist. Übertragen auf die Automatisierungstechnik wäre es daher nicht ratsam, Sicherheit erst in der Steuerung realisieren zu wollen. Vielmehr muss das Umfeld, in denen Steuerungen und Web-Panel zum Einsatz kommen sicher ausgestaltet sein.

Generell lässt sich Sicherheit in IT-Anwendungen in zwei Themenbereiche unterteilen: dem unerlaubten Eindringen in Rechner- und Netzwerksysteme (Hacking) und Viren. Viren bauen auf eine möglichst weit verbreitete HW-Plattform mit Standardbetriebssystem, wie es eben Windows®-PCs darstellen. Eine Steuerung ist in der Regel mit optimierten Mikrocontrollern bzw. Prozessoren aufgebaut und mit einem proprietären Betriebssystem ausgestattet. Damit sind sie immun gegenüber allen für PCs und Windows® geschriebenen Viren. Die im Vergleich zu PCs geringe Verbreitung von Steuerungen macht es auch äusserst unwahrscheinlich, dass spezielle Viren für Steuerungssysteme auftauchen. Theoretisch sind Windows®-basierte Bedienpanel da anfälliger. Virenentwickler wollen einen möglichst grossen Effekt erzielen und setzen daher auf die Desktop-Betriebssysteme Windows® 2000/XP/Vista. Windows® CE ist da schon weit weniger attraktiv. Weiter ist zu beachten, dass Viren hauptsächlich durch den Anwender selbst eingeschleppt und aktiviert werden. Das kann schnell durch einen Klick zuviel beim Internet-Surfen oder durch die Installation eines verseuchten Programms passieren. Bedienpanel in industriellen Anwendungen sind meistens geschlossen; d.h. eine Bedienoberfläche wird automatisch beim Booten gestartet und der Bediener hat gar keine Möglichkeit, kritische Web-Seiten anzusteuern oder gar Software zu installieren.

Wer insbesondere bei Windows® XP basierten Panel auf Nummer sicher gehen will, kann einen Viren-Scanner installieren. Man sollte dann aber einen Scanner wählen, welcher sich automatisch mit den neuesten Virensignaturen aktualisiert und seinen Dienst diskret im Hintergrund ohne nervige Popup-Fenster und erzwungener Benutzerinteraktion verrichtet. Hier versagen leider die meisten handelsüblichen Viren-Scanner. Dass es auch anders geht beweist die Firma Eset® (www.eset.com) mit ihrem Produkt Nod32. Nod32 lässt sich komplett ohne Benutzerinteraktion in einem so genannten «stillen Modus» betreiben und versendet sogar E-Mails, wenn eine Infektion erkannt wurde.

Im Vergleich zur Virengefahr muss dem Hacking in industriellen Anwendungen ein wesentlich höherer Stellenwert eingeräumt werden. Insbesondere bei Web-Visualisierungen, bei denen sozusagen die gesamte Bedienoberfläche frei Haus geliefert wird, ist eine solide Zugangskontrolle notwendig. Dies kann durch einen vorgeschalteten Proxy-Server mit Authentifizierung erreicht werden. Vom Internet eingehende Anfragen werden zunächst auf den Proxy-Server geleitet. Bevor der Proxy-Server die Anfrage an die entsprechende Steuerung weiterleitet muss der Benutzer sich mit einer Benutzer/Passwort-Kennung anmelden (Authentifizierung). Dadurch ist sichergestellt, dass nur eine bestimmte Personengruppe Zugang erhält. Will man sich auch gegen «Lauschangriffe» (Sniffer) schützen, kann der Proxy-Server auch eine SSL-Verschlüsselung des kompletten Datenverkehrs vornehmen. Damit erzielt man denselben Sicherheitslevel wie bei Web-Shops und Online-Banking.
Eine weiter Methode zur Zugangskontrolle stellt VPN (Virtual Private Network) dar. Hierbei werden private Daten über das Internet in einem so genannten Tunnel übertragen. Die Übertragung kann verschlüsselt werden. Über eine VPN-Tunnel können Anwender auf Rechner über das Internet auf dieselbe Art zugreifen, als ob sie sich in einem LAN befänden. Für den Zugriff auf ein VPN muss ein Software-Client auf dem Rechner (PC) installiert sein, der dann die Verbindung herstellt.Um nun in den Genuss der oben beschriebenen Sicherheitstechniken zu kommen, ist es nicht unbedingt notwendig einen ausgewachsenen Server-PC einzusetzen. Auf dem Markt sind dafür kompakte, für den Einsatz im Schaltschrank konzipierte Geräte erhältlich. Beispielsweise bietet die Firma Eurogard (www.eurogard.de) einen preiswerten Service-Router an, der einen Proxy-Server mit SSL-Verschlüsselung und VPN bietet und speziell auf PCD-Steuerungen von Saia-Burgess Controls ausgerichtet ist.



Durch Proxy-Server gesicherter Zugang zum Internet für Web-Panel und Steuerungen.

Saia-Burgess Controls AG
Bahnhofstrasse 18 | 3280 Murten, Schweiz
T +41 26 672 72 72 | F +41 26 672 74 99
www.saia-pcd.com

support@saia-pcd.com | www.sbc-support.com

P+P26/261 DE03 02. 2014 Änderungen technischer Daten und Angaben vorbehalten.