

SECURITY KIT SK/92: DIE DETAILS ZUR FUNKTIONSWEISE

Dieses White Paper beschreibt die typische zellenförmige Infrastruktur beim Ethernet-Einsatz in der Automatisierung und die Sicherheitsrisiken durch Webserver in Automatisierungsbaugruppen. Es liefert weiterhin einen Einblick, wie derartige Schwachstellen durch den Einsatz des IGW/920-basierten Security Kit SK/92 zu beseitigen sind.

1. Die Netzwerkinfrastruktur

Ethernet LANs in der Automatisierung werden im Allgemeinen in separate Zellen unterteilt. Eine solche Zelle kann aus einem einzigen Schaltschrank, einer Gruppe von Schaltschränken oder sogar einer ganzen Fabrikhalle bestehen (aus dem Betrachtungswinkel der Sicherheit gilt: je kleiner die einzelne Zelle, desto besser kann sie geschützt werden). In eine solche Netzwerkzelle sind dann alle Automatisierungsbaugruppen mit Ethernet-Schnittstelle direkt oder über so genannte Device Server (spezielle Protokollkonverter mit Ethernet auf der einen und RS-232- oder Feldbusschnittstellen auf der anderen Seite) eingebunden.

Die LAN-Zelle selbst besitzt aus Sicherheitsgründen in der Regel nur eine einzige Verbindung zu anderen IP-basierten Netzwerken. An den Zellenübergängen findet man in zahlreichen Installationen bereits seit einigen Jahren Firewalls, um die einzelnen Systeme – soweit möglich – vor unerlaubten Zugriffen zu schützen. Teilweise kommen neuerdings auch spezielle Automatisierungs-Router zum Einsatz, die die Funktionen einer Firewall und eines LAN-Switches in einem einzigen Gerät vereinen.

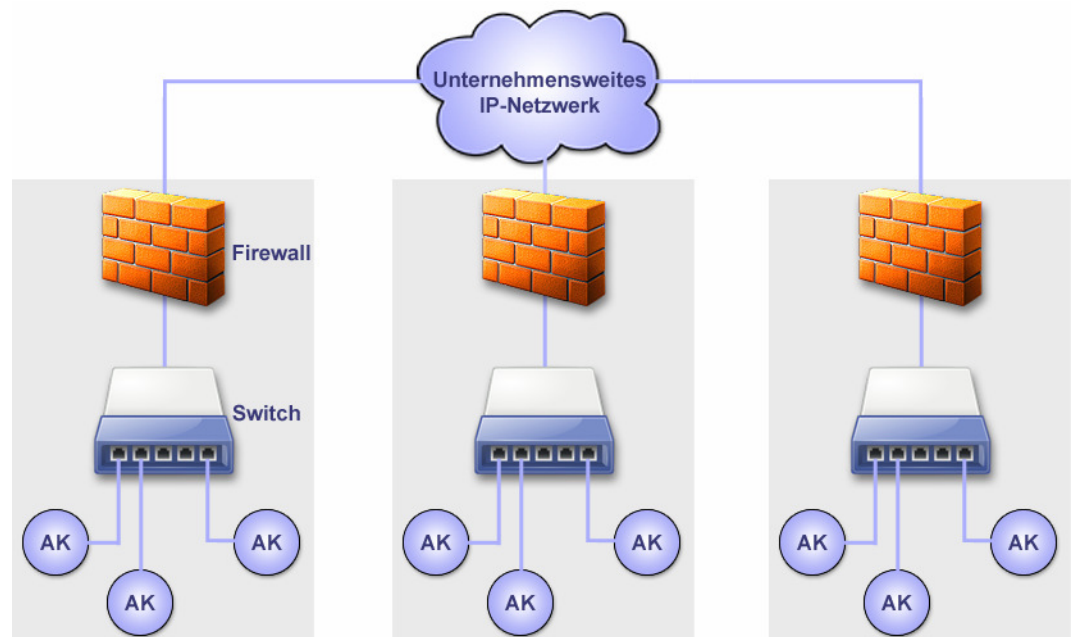


Abb. 1: Zellenstrukturen in der Automatisierung

Es soll in der Praxis aber auch noch unternehmensweite Ethernet-LANs geben, in denen die IT-Systeme und Automatisierungsbaugruppen eines Unternehmens ohne jegliche Zellenbildung in einem einzigen gemeinsamen Netzwerk betrieben werden. Derartige Konstellationen sind nach aktuellen Sicherheitsaspekten als sehr kritisch einzuordnen. Besonders dann, wenn ein solches Unternehmens-LAN auch noch einen Zugang zum Internet besitzt, um den Mitarbeitern die IP-Kommunikation (E-Mail-Ein- und Ausgang, Webzugriffe, VoIP usw.) mit dem Rest der Welt zu ermöglichen.

2. Das Problem

In einem Industrial Ethernet LAN findet man zahlreiche Baugruppen, die einen eingebetteten (Embedded) Webserver besitzen. Diese Benutzerschnittstelle dient zur Gerätekonfiguration und Statusabfrage. Um eine solche HMI-Schnittstelle zu nutzen, muss auf einem PC nur ein Webbrowser gestartet und die IP-Adresse der jeweiligen Baugruppe als Adresse eingetippt werden. Teilweise ist dann auf der Baugruppen-Homepage noch ein spezielles Passwort einzugeben, um den vollständigen Schreib/Lese-Zugriff auf sämtliche Parameter der einzelnen Konfigurationsseiten zu erhalten (wichtiger Hinweis: ein derartiger Passwortschutz über eine spezielle Login-Webseite ist kein ernstzunehmender Sicherheitsbaustein zum Schutz vor unerlaubten Zugriffen, sondern bestenfalls ein Alibi).

Durch die unternehmensweite Vernetzung auf Basis von Ethernet und TCP/IP kann der Anlagenbetreuer (aber leider auch jeder andere Nutzer) von jedem beliebigen Standort innerhalb des Firmen-LANs auf die Webseiten einer Automatisierungsbaugruppe zugreifen und – wenn gewünscht – auch Veränderungen der Gerätekonfiguration durchführen. Teilweise sind die Industrial-Ethernet-LAN-Zellen direkt oder indirekt mit dem Internet verbunden. Dann kann sogar aus der Ferne – also praktisch von jedem beliebigen Ort auf dieser Welt aus – zwecks Teleservice (Remote Access zu Servicezwecken) auf die einzelnen Webserver einer Zelle zugegriffen werden. Mit Hilfe spezieller Namensdienste, wie zum Beispiel DynDNS [Dyn] und einem für derartige Fernzugriffe konfigurierten Router, ist dann nicht die lokale IP-Adresse der Automatisierungsbaugruppe in der LAN-Zelle, sondern ein entsprechender (DNS-) Name als Adresse erforderlich.

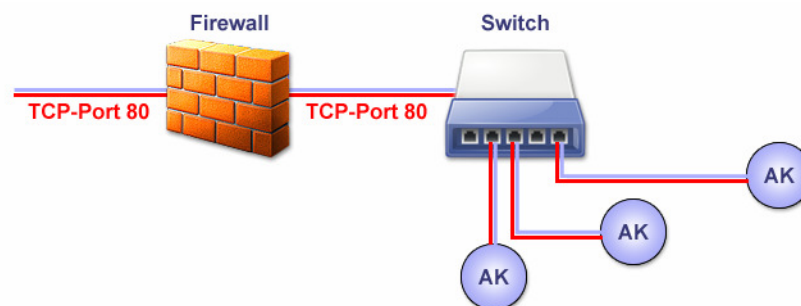


Abb. 2: Firewall mit TCP-Port 80 zu allen Baugruppen

Um Web-basierte Zugriffe auf Automatisierungsbaugruppen zuzulassen, muss die Firewall an der Verbindung einer Automatisierungs-Zelle zur Außenwelt entsprechend konfiguriert werden. Der Datenverkehr zum TCP-Port 80 (HTTP) – das ist die logische Schnittstelle, unter welcher ein Webserver für die Anfragen eines Browser erreichbar ist – muss die bidirektionale Kommunikation erlauben. Die Zugriffe auf alle anderen TCP-Ports [Wal], wie zum Beispiel Telnet, FTP usw. können durch die Firewall unterbunden werden. Die jeweiligen Ports sind dann durch die Firewall-Konfiguration für alle externen Zugriffe gesperrt.

Nur innerhalb der Industrial-Ethernet-LAN-Zelle ist die Nutzung dieser TCP-Ports dann noch gestattet. Grundsätzlich gilt: eine Firewall, die den TCP-Port 80 nicht blockiert, stellt ein sehr großes Sicherheitsrisiko dar. In sicheren IT-Netzwerken gibt es derartige Schwachstellen im Allgemeinen nicht, da Webserver immer außerhalb normaler Netzwerke positioniert werden, bzw. die Webserver innerhalb eines LANs von außen nicht erreichbar sind. Darüber hinaus werden für alle Nutzer erreichbare Webserver in IT-Anwendungen nicht zur Konfiguration per Webbrowser, sondern lediglich als Informationsquelle genutzt.

Grundsätzlich ist jeder Embedded Webserver in einem Industrial Ethernet LAN, der die Konfiguration eines Systems per Browser zulässt, als sicherheitstechnische Schwachstelle anzusehen. Die Ursachen für die Sicherheitslücken sind in erster Linie direkt in den Grundideen und -konzepten der zum Einsatz kommenden Protokolle zu suchen. Von Haus aus übertragen TCP/IP und Co. die Nutzdaten im Klartext. Weder TCP und UDP in der Transportschicht eines typischen Protokollstacks, noch IP in der Vermittlungsschicht bieten standardmäßig eine Verschlüsselung. Sämtliche Daten, die von Applikationsprotokollen wie HTTP an TCP und somit auch an IP übergeben werden, laufen praktisch im Klartext über das Übertragungsmedium. Mit entsprechenden Werkzeugen, wie zum Beispiel einem LAN-Sniffer, kann die Kommunikation aufgezeichnet und ausgewertet werden. Dabei sind dann auch geheime Passwörter und sonstige vertrauliche Daten für jedermann lesbar.

Weiterhin bleiben die tatsächlichen Kommunikationspartner bei einer TCP/IP-Übertragung anonym. Der Sender einer Nachricht kennt den wahren Empfänger nicht und umgekehrt. Eine Authentifizierung ist standardmäßig nicht vorgesehen. Problematisch ist auch die Datenintegrität. Werden auf dem Weg zwischen Sender und Empfänger die Daten absichtlich verändert, bleibt dies in der Regel unerkannt.

3. Die Schutzfunktion des Security Kit SK/92

Der zuvor beschriebenen Problematik der ungesicherten Web-basierten Zugriffe auf Automatisierungsbaugruppen kann sehr einfach begegnet werden. Statt den direkten Zugriff auf die einzelnen Webserver zuzulassen, wird ein entsprechender Sicherheits-Proxy (Stellvertreter-Server mit Schutzfunktionen) in die jeweilige Zelle eingebracht, der ausschließlich über einen VPN-Tunnel (VPN = Virtual Private Network) erreichbar ist. Der Webzugriff durch externe Nutzer erfolgt dann nur noch auf den Web-Proxy-Server. Dieser setzt die externen Zugriffe dann innerhalb der Zelle in Standard-HTTP-Zugriffe um, so dass an der TCP/IP- und Softwarekonfiguration der einzelnen Automatisierungsbaugruppen nichts verändert werden muss (genau genommen bekommen diese Baugruppen von der Existenz des Proxy überhaupt nichts mit).

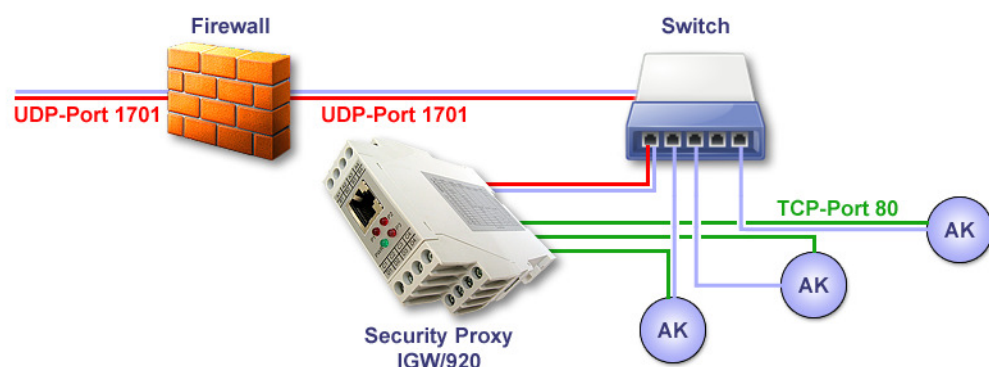


Abb. 3: Firewall mit UDP-Port 1701 zum IGW/920

Die Firewall einer Industrial-Ethernet-LAN-Zelle als Schnittstelle zur Außenwelt ist dann so zu konfigurieren, dass alle TCP-Ports für Zugriffe von außerhalb geschlossen sind. Lediglich ein einziger UDP-Port (zum Beispiel 1701) wird über die Konfigurationseinstellungen geöffnet. Dieser ist direkt mit der VPN-Software des Sicherheits-Proxy verbunden. Sämtliche Zugriffe auf die Webserver in den Automatisierungsbaugruppen erfolgen dann durch den VPN-Tunnel. Ein derartiger Tunnel bietet die drei wichtigsten Sicherheitsgrundbausteine für zeitgemäße Kommunikationsverbindungen: 1. Vertraulichkeit (Datenverschlüsselung), 2. Integrität (Schutz gegen Datenverfälschungen) und 3. Authentizität (sichere Zuordnung empfangener Daten zum Sender und der Nachweis, dass sie tatsächlich von diesem Sender stammen).

Der Device Server IGW/920 im Security Kit SK/92 ist für den Einsatz als Sicherheits-Proxy vorbereitet. Dieser spezielle Hutschienen-Server wird mit vorinstallierter OpenVPN-Software [OpV] und einem Reverse Proxy mit dem Namen Pound [Pou] ausgeliefert. Mit Hilfe von OpenVPN werden die Sicherheitsgrundbausteine realisiert. Pound dient zur Implementierung der Proxy-Funktionen. Diese Softwarekomponente erhält als Konfigurationsdaten die IP-Adressen der Automatisierungsbaugruppen mit Webserver. Jedem einzelnen Server wird für den Zugriff durch den VPN-Tunnel eine frei wählbare Portnummer zugeordnet. Dabei entsteht dann ein Mapping wie zum Beispiel in der Tabelle 1 dargestellt.

IGW/920 TCP-Port	Zielsystem in der Automatisierungszelle
1024	192.168.0.100:80 (Webserver in der SPS 1)
1025	192.168.0.145:80 (Webserver im Modbus Device Server)
1026	192.168.0.155:80 (Webserver im CAN/LAN Gateway)
1027	192.168.0.212:80 (Webserver in der SPS 2)

Tabelle 1: Beispiel einer Mapping-Tabelle für den Sicherheits-Proxy

Die zum Einsatz kommende OpenVPN-Software realisiert ein so genanntes SSL-VPN. Derartige VPNs können – im Gegensatz zu den IPsec-basierten Vertretern – nachträglich ohne spezielle Kenntnisse und den Austausch von Routern in jedes IP-basierte Netzwerk eingebracht werden. Auf den PCs, die zukünftig über den Proxy auf die Automatisierungsbaugruppen zugreifen sollen, ist allerdings ein VPN-Client erforderlich. Für OpenVPN steht diese Softwarekomponente für alle gängigen PC-Betriebssysteme kostenlos im Internet [OpV] zur Verfügung. Um die Authentizität eines bestimmten PCs als Kommunikationspartner im VPN zu gewährleisten, werden Zertifikate (Zertifikatsdateien) benutzt. Über ein solches Zertifikat wird einem bestimmten PC der Zugriff auf das VPN gestattet und bei Verlust der Berechtigung auch wieder entzogen. Das jeweilige Zertifikat wird dann einfach für ungültig erklärt.

Quellenangaben

[Dyn] Website zu DynDNS: www.dnyns.com

[OpV] Website und Download zu OpenVPN: www.openvpn.net

[Pou] Website zu Reverse Proxy und Load Balancer Pound: www.apsis.ch/pound

[Wal] Walter: Embedded Internet in der Industrieautomation. Hüthig, Heidelberg 2004.

Kontakt

SSV Embedded Systems

Heisterbergallee 72

D-30453 Hannover / Germany

Phone: +49 (0)511/40 000-0

Fax: +49 (0)511/40 000-40

E-mail: sales@ist1.de

Internet: www.ssv-embedded.de

Dokumenthistorie

Revision	Datum	Bemerkungen	Name
0.1	2008-11-17	erste version	KDW

Dieses Dokument ist nur für die interne Verwendung bestimmt. Der Inhalt dieses Dokuments kann sich jederzeit ohne Ankündigung ändern. Es wird keine Garantie für die Richtigkeit der Angaben übernommen. Einige in der dieser Beschreibung erwähnte Produkt- und Firmennamen sind möglicherweise die Warenzeichen der jeweiligen Besitzer.

© 2008 SSV EMBEDDED SYSTEMS und Klaus-Dieter Walter. Alle Rechte vorbehalten.