

# Brücken bauen

Sichere Prozessdatenvisualisierung auch über's Internet

B&B Security  
Produktreport

*Sicherheit ist ein Muss im Unternehmensnetzwerk – auch wenn es manchmal mit dem Umsetzen hapert. Es ist verständlich, dass eine übers Intranet oder Internet verteilte Prozessdatenvisualisierung zwiespältig betrachtet wird. Der Grund dafür: das höhere Risiko nicht-authorisierter Zugriffe auf das IT- oder Produktionsnetzwerk des Betriebes. Gefahren, die sich schon mit geringem Aufwand auf ein Minimum reduzieren lassen.*

Simone Henseler

Das große „ABER“... es tritt genau dann auf, wenn man zwei Netzwerke miteinander koppeln will. Denn, wie sieht es in der Fabrik oder im Büro aus? Daten sammeln, Informationen generieren, ob Füllstände, Temperaturen oder Verbrauchswerte, die Visualisierungssysteme müssen die Vielzahl der Prozessdaten in den Griff bekommen. Um diese Datenflut eindeutiger und transparenter darstellen zu können, sollte man die Informationen bedarfsgerecht verarbeiten. Visualisierungssysteme basieren oft auf In-sellösungen, entsprechende Daten erreichen nicht immer den richtigen Mitarbeiter. Und: Verschiedene Personengruppen haben auch einen unterschiedlichen Informationsbedarf. Komplexe Abläufe einfach darstellen kann inMOVE, die Visualisierung der Inray Industriesoftware GmbH.

In der Praxis gilt: Einen Instandhalter in der Produktion interessieren mehr die Zustände der Maschinen als die Verbräuche von Ma-

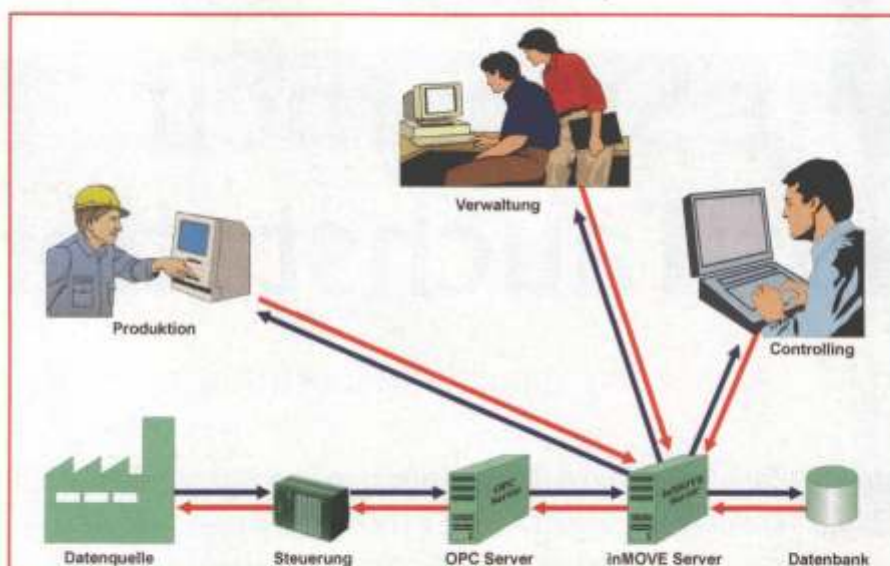
terialien. Wiederum sind die Maschinenzustände für das Büro weniger von Bedeutung, dagegen der Materialverbrauch umso mehr, damit eine Nachbestellung schnellst möglich erfolgen kann. inMOVE macht sich modernste Webtechnologien zunutze, damit die entsprechenden Daten die richtigen Personen erreichen. Dies geschieht ganz einfach – nämlich per MS-Internet Explorer.

## Security-Techniken, schaffen Sicherheit

Die meisten Unternehmen trennen das Netzwerk für die Produktion und das für die IT, beide arbeiten oft voneinander getrennt und autark. Dies ist durchaus sinnvoll, damit keine unbefugten Zugriffe auf die Steuerungen erfolgen. Der Alltag für Mitarbeiter aus der Verwaltung aber sieht oft wie folgt aus: Er benötigt die aktuellen Materialbe-

stände, ruft deshalb laufend im Lager an, oder er muss gar laufen, um dies herauszufinden. Oder der Instandhalter! Er vernimmt zwar ein ungewöhnliches Maschinengeräusch, aber er weiß nicht, woher es kommt und was die Ursache. Hier bildet die Visualisierung eine Brücke zwischen beiden Netzwerken. Mit ihr lassen sich die aktuellen Materialbestände bequem vom Arbeitsplatz - via Internet Explorer - aus abrufen. Zudem lässt sich auch das Maschinengeräusch zuordnen sowie der Auslöser des Alarms ermitteln. Warum also nicht beide Netzwerke einfach miteinander koppeln? Und das, ohne eine Brücke zu schaffen! Und damit sei das Problem gelöst. Doch dann kommt es, das große „ABER“! Wenn man beide Ebenen, die Ebene des Büros und die der Fabrik, sorglos miteinander verbindet, entstehen Sicherheitslücken. Man denke nur an das Stehlen oder Zerstören von betriebsin-

Dipl.-Ing. Simone Henseler ist Mitarbeiterin der Inray Industriesoftware GmbH, Schenefeld.



Die Visualisierungslösung InMove kanalisiert und verteilt Prozessdaten im Unternehmen.

ternen Daten. Auch die verheerenden Folgen eines Angriffs auf eine Fertigungsstraße lassen sich leicht ausmalen: wenn die Fertigungsroboter mit den Produkten um sich werfen, die sie eigentlich produzieren sollten. Es drohen jedoch nicht nur Gefahren von außen, sondern auch von innen. Befugte Benutzer können durch unwissentliches Installieren schädlicher Software oder das Anzeigen von ungefilterten E-Mails und Webseiten das Netzwerk in Mitleidenschaft ziehen. Bei solchen Sicherheitsdefiziten können die daraus resultierenden Konsequenzen harmlos sein, aber auch verheerend. Ein nicht autorisierter Zugriff auf die Steuerung kann Produktionsstillstand verursachen oder Menschen gefährden.

Man kann dem aber entgegenwirken, indem man eine von den vielen angebotenen Security-Technologien nutzt – beispielsweise OpenVPN (Virtual Private Network). Damit lassen sich Informationen geschützt über öffentliche Netze übertragen. OpenVPN funktioniert so:

- ▶ die Verbindung mit dem Intranet aufbauen,
- ▶ die Verbindung zum OpenVPN-Server, der eine Authentisierungsprüfung durchführt,
- ▶ eine gesicherte Datenverbindung wird erstellt (auch Tunnel genannt) und
- ▶ die verschlüsselten Daten werden übermittelt und wieder entschlüsselt.

Ein Bild verdeutlicht den Vorgang: von Arbeitsplatz zu Arbeitsplatz lässt sich ein Tunnel erzeugen, durch den die Daten fließen. Deshalb nennt sich diese Methode auch End-To-End. Weil aber VPN für virtuelles privates Netzwerk steht, können weitere Nutzer miteingebunden werden. Zwei un-

terschiedliche Arten von Schlüsseln chieffrieren und dechiffrieren die Daten. Zum einen gibt es die symmetrischen Schlüssel. Hier verwendet man ein- und denselben Schlüssel. Von Nachteil dabei: Wird einer der Schlüssel bekannt, ist kein sicherer Datenaustausch mehr möglich. Der Vorteil: Er liegt im schnellen Ver- und Entschlüsseln. Zum anderen gibt es die asymmetrischen Schlüssel: Dabei setzt man auf das Verwenden unterschiedlicher Schlüssel, den sogenannten Schlüsselpaaren. Diese bestehen aus einem privaten und einem öffentlichen Teil. Der Vorteil: Die Schlüssel lassen sich leichter austauschen. Welchen Schlüssel man nun verwendet, das kommt ganz auf

die Einzelsituation an. Ratsamer ist sicherlich die asymmetrische Verschlüsselung, weil diese sicherer ist und auch von vorneherein von OpenVPN angeboten wird. Dabei entsteht eine SSL-verschlüsselte Verbindung. SSL steht für Secure Socket Layer und ist ein Protokoll zum Übertragen für verschlüsselte Informationen. SSL wurde für den Einsatz zwischen Client und Server entwickelt. Das Protokoll besteht im wesentlichen aus drei Teilen:

- ▶ dem Record-Protokoll: Es gibt die angewandten Verschlüsselungs- und Authentifizierungsfunktionen an,
- ▶ dem Handshake-Protokoll: Mit diesem Protokoll behandeln Client und Server den Einsatz von kryptografischen Algorithmen und Schlüsseln und
- ▶ dem Alert-Protokoll: Es meldet Fehler und/oder das Ende der Kommunikation.

OpenVPN, eine freie Software, ist eine der zahlreichen Möglichkeiten, sich vor unbefugten oder auch befugten Zugriffen in einem Netzwerk sicher schützen zu können. Es sollte nicht als generelle und bestmögliche Lösung gesehen werden. Es sollte lediglich eine Vorstellung für die Problemlösung sein. Das große „ABER“ ... also auch hier: Die Security-Techniken sind vorhanden – aber man muss sie nutzen. (klu)

Inray Industriesoftware  
Tel. +49(0) 4892 80170

[www.elektrotechnik.de](http://www.elektrotechnik.de)  
Visualisierung im Web  
OpenVPN - die Technologie

Info-Click

177933

## Industriernetzwerke: die vier Feinde!

Computer und Daten in einem Netzwerk haben vier potenzielle Feinde:

- Feind 1: Fehler, die durch die Technik selbst ausgelöst werden. (Beispiel: Rechnerabsturz, brauche dringend Hilfe!)
- Feind 2: Fehler, die durch unvorhersehbare Ereignisse entstehen. (Beispiel: Großbrand legt Produktion lahm)
- Feind 3: Fehler, die durch unbefugte Zugriffe ausgelöst werden. (Beispiel: Sasser-Wurm-Programmierer gefasst!)
- Feind 4: Fehler, die durch befugte Benutzer ausgelöst werden. (Beispiel: Viren, Würmer und Trojaner)