

A woman in a light blue shirt and dark trousers is pushing a large white puzzle piece from the left. A man in a dark suit is pushing a large white puzzle piece from the right. The puzzle pieces are set against a rough, grey stone wall. The scene is lit from the side, creating strong shadows.

IT-Systeme in Verwaltung und Produktion  
intelligent verbinden

## Zusammen – und doch jedem das Seine

**Produzierende Unternehmen stellen besondere Ansprüche an die Sicherheit der eingesetzten IT-Technologie, denn sie betreiben unterschiedliche Netzwerke mit höchst unterschiedlichen Anforderungen. Was in der Verwaltungs-IT sinnvoll ist, kann in der Produktion verheerende Folgen nach sich ziehen. Hohe Sicherheitsstandards im Office-LAN können beispielsweise die Wartung an Maschinen und Anlagen im Produktions-LAN behindern. Dennoch müssen beide Netze, Verwaltung und Fertigung, miteinander kommunizieren. Wie eine intelligente Verbindung zwischen Office- und Produktions-LAN auszusehen hat, um einen ausreichenden Schutz sensibler Daten einerseits und schnelle Reaktionsmöglichkeiten bei denkbaren Ausfällen andererseits zu bieten, darüber streiten sich die Experten. Folgender Beitrag gibt einen Einblick in Lösungsstrategien, wie sich Verwaltungs- und Produktions-IT sinnvoll miteinander verbinden lassen.**

Am Beispiel geltender Sicherheitsstandards wird das Problem deutlich: In der Produktion arbeiten Unternehmen häufig mit lokalen Administratorenrechten oder lokalen Profilen. Der Einsatz strenger Kennwortrichtlinien, wie man sie aus der Office-IT kennt, ist nahezu unmöglich, da ständig wechselnde Mitarbeiter die Maschinen und Anlagen bedienen. Hinzu kommt die Tatsache, dass für die Wartung betriebsfremde Personen auf die Produktionsanlagen zugreifen. Während es gerade in Sachen Sicherheit auch auf die Aktualität der eingesetzten IT-Technologie ankommt, lässt es sich in der Produktion oftmals nicht vermeiden, dass Maschinen und Anlagen mit veralteten Betriebssystemen laufen. Teilweise verlangen die Hersteller sogar den

Einsatz alter Softwareversionen, da ansonsten keine Funktionen genutzt werden können oder Patches unmöglich ist. Dementsprechend geben sie keine Gewährleistung oder verweigern die Zertifizierung, wenn ein Unternehmen ein aktuelleres Betriebssystem nutzen will. Jenes gerät in die Zwickmühle, wenn es auch für das Produktions-LAN hohe Sicherheitsstandards halten will – immerhin ist die Installation zum Beispiel eines 500 MByte großen Virenschutzes auf ein Windows-95-System mit gerade einmal 4 MByte RAM schwerlich machbar. Wie lässt sich also sicherstellen, dass sich Störungen in einzelnen Systemen nicht auf die gesamte Produktion auswirken? Wie kann der externe Zugriff auf Maschinen und der Zugang zu einzelnen Netz-

abschnitten für das Wartungspersonal sicher gestaltet werden?

### Verfügbarkeit, Integrität, Datenschutz

In der Verwaltung werden Dateien von zentralen Servern bereitgestellt, die auf Büro-IT-Systemen bearbeitet und wieder auf diesen Servern abgelegt werden. Zudem brauchen die Mitarbeiter hier Zugriff auf zentrale Lösungen wie zum Beispiel das ERP- (Enterprise Resource Planning) oder das Finanzbuchhaltungssystem. Typisch für ein Office-Netzwerk ist auch ein hohes Maß an interner und externer Kommunikation. Der Fokus liegt demnach auf der Bereitstellung von Informationsspeichern, dem Austausch von Daten sowie dem Zugriff auf informationsverarbeitende Systeme. Durch eine weitgehend standardisierte Systemlandschaft im Office-Umfeld setzen Unternehmen Standardwerkzeuge für Firewall, Virenschutz, Patchmanagement, Remotezugriff und Administration ein. Die genutzten Endgeräte sind meist einzelnen oder wenigen Mitarbeitern zugeordnet. Steht eine Aktualisierung der Systeme an, können Hard- und Software abteilungs- oder unternehmensweit ausgetauscht werden. Kurzfristige Betriebsunterbrechungen oder zeitweise verzögerte Reaktionszeiten sind meist nicht unternehmenskritisch. Im-

merhin gilt im Office-LAN das Kürzel CIA: Confidentiality, Integrity, Availability.

In der Produktion kehrt sich die Reihenfolge jedoch um: Hier steht Availability an erster Stelle – und quasi auch an zweiter und dritter. Denn im Vergleich zur Verwaltung spielen Integrität und Sicherheit derzeit eher eine untergeordnete Rolle (AIC statt CIA). In den verschiedenen Produktionsanlagen laufen unterschiedliche IT-Systeme mit vielfältigen Betriebssystemvarianten. In ihrer Konfiguration sind sie fixiert, da ansonsten keine Gewährleistung geboten wird. Die Softwarelösungen sind individuell konzipiert, die Kommunikationsprotokolle sind uneinheitlich. Oftmals sind die Systeme hinsichtlich Verfügbarkeit und vor allem in Bezug auf die Performance der Kommunikationswege sehr sensibel. Also liegt der Fokus in der Produktion bei einer höchstmöglichen Verfügbarkeit und Performance. Sicherungsmaßnahmen, wie sie nun notwendig werden, dürfen diese Parameter nicht negativ beeinflussen. Darüber hinaus müssen sie mit einer heterogenen Systemlandschaft harmonisieren und dennoch höchstmöglichen Schutz bieten.

### Trennen, unterteilen und kontrollieren

Ein möglicher Lösungsansatz liegt in der Etablierung eines Schutzkonzeptes mit vielen Schichten – dem Defense in Depth –, beginnend mit dem physischen Zutritt zu den Anlagen über die Netzwerksicherheit (Trennung von Produktion und Verwaltung, tiefengestaffelte Sicherheitsarchitektur mit weiterer Segmentierung des Netzes etwa nach ISA 99) bis hin zum Zugriffsschutz. Die Trennung von Verwaltung und Produktion erfolgt durch die Unterteilung des physischen Netzwerks in zwei logische Teilnetze mittels VLAN oder durch den Einsatz einer Firewall zwischen den in diesem Fall dann physisch getrennten Netzen. Aufgrund der genannten Anforderungen und der angestrebten Topologie erscheint der Einsatz einer großen Firewall mit der physischen Trennung der Netze als sinnvollere Lösung, da VLANs aus Sicht des Sicherheitsmanagements oftmals schwerer zu kontrollieren sind.

Der nächste Schritt ist die Segmentierung des Produktions-LAN in einzelne Teilnetze, beispielsweise über ein Zellschutzkonzept. Hierbei werden einzelne Automatisierungszellen etabliert, innerhalb derer organisatorisch eng verzahnte Geräte miteinander kommunizieren können. Der Zugang zu einem Teilnetz wird wiederum durch eine dezentrale (Industrie-)Firewall abgesichert. Der Kommunikationsweg zu anderen Automatisierungszellen oder externen Ressourcen kann dabei zusätzlich über VPN-Kanäle erfolgen. Als eine weitere Stufe der Sicherung kann zwischen Produktion und Verwaltung neben der großen Firewall noch eine DMZ (Demilitarisierte Zone, eine Art neutrale Pufferzone) eingerichtet werden, um den direkten Informationsfluss zwischen Geräten aus der Produktion, der Verwaltung und externen Systemen zu unterbinden.

### Segmentierung mit Automatisierungszellen

Um den Anforderungen einer kontrollierten Kommunikation zwischen einzelnen Office-Systemen und Geräten in der Produktion gerecht zu werden, bieten sich unterschiedliche Lösungsansätze an. Mittels VPN-Tunnel können Systeme aus dem Verwaltungsnetzwerk gezielt mit Geräten in einer bestimmten Automatisierungszelle kommunizieren. Ebenfalls denkbar ist die Nutzung von dezentralen Firewall-Routern im Eingangsbereich des Teilnetzes, die ein 1:1-NAT (Network Address Translation, Übersetzung der Netzwerkadressen) ermöglichen.

Auch für die Fernwartung sind Unternehmen mit einer solchen Netzarchitektur gerüstet. Der gezielte, externe Zugriff in eine Automatisierungszelle via VPN-Tunnel vereinfacht nicht nur die Administration, sondern ermöglicht auch die detaillierte Protokollierung der Aktivitäten. Kommt es dennoch zum Störfall, ist maximal die einzelne Automatisierungszelle betroffen. Die Segmentierung begrenzt auch das Risiko auf die einzelne Zelle, wenn externes Wartungspersonal vor Ort mit eigener IT auf die Produktion zugreift. In kritischen Situationen können die Regeln und Einschränkun-

gen des Übergangspunktes auch während der Wartung verschärft werden und das System nach Abschluss der Wartungsarbeiten zunächst einer eingehenden und lokal beschränkten Kontrolle unterzogen werden. Wichtig bei der Auswahl der Firewall- und Routersysteme bleibt die Möglichkeit einer zentralen Verwaltung durch ein Zentralmanagement, denn der Einsatz von Automatisierungszellen geht mit einer Vielzahl von Übergangspunkten einher. Bei der Aufgabe, Geräte und Netze zu überwachen, erweist sich die Segmentierung erneut als großer Vorteil. Unterschiedliche Systeme können mit individuell anpassbaren Monitoring-Lösungen lokal überwacht und die Resultate dann an ein zentrales SIEM (Security Information and Event Management) zur globalen Darstellung und Auswertung zurückgemeldet werden.

### Fazit

Durch ein vielschichtiges Schutzkonzept können Unternehmen aus dem Office-LAN auf die Produktion zugreifen, ohne dass sie dabei auf die nötigen Sicherheitsstandards verzichten müssen. Im Gegenteil: Die Anwendung segmentierter Netzwerke erleichtert die Administration und sorgt dafür, dass sich etwaige Störungen nur lokal und nicht auf die gesamte Produktion auswirken. Mittels dieser Segmentierung können das Produktions-LAN und die dort eingesetzte IT effizient geschützt werden, da unterschiedliche Schutzsysteme in den Automatisierungszellen unabhängig voneinander etabliert werden können. ■



STEFAN SCHAFFNER,  
Geschäftsführer, ASS it-systemhaus GmbH



Für Abonnenten ist dieser Artikel auch digital auf [www.datakontext.com](http://www.datakontext.com) verfügbar