

Viren in Werkzeugmaschinen?

Seit langem werden die Gefahren, die von Viren und Würmern im Büroumfeld ausgehen, diskutiert und mittels vielseitiger organisatorischer und technischer Maßnahmen bekämpft. Anders stellt sich die Situation in Bereich industrieller Kommunikation dar.

Von **Olaf Siemens, Berlin**

Aus der Bürokommunikation bekannte Standards wie Ethernet und TCP/IP verbreiten sich sehr schnell auch in Anwendungen in der Fertigungsautomation, der Prozessautomation, der Vernetzung von Geldautomaten, Point of Sales-Terminals und der Fernwartung und des Fernwirkens. Die Begeisterung für eine unternehmensweite Vernetzung ist groß. Noch ist vielen Verantwortlichen nicht klar, dass die Verbreitung der Standardprotokolle auch die Netzwerksicherheit in den hinzukommenden Bereichen auch gefährden kann, denn mit dem Zusammenwachsen der bislang mit unterschiedlichen Protokollen arbeitenden „IT-Inseln“, fallen auch die Grenzen für Viren und Würmer.

Das mangelnde Sicherheitsbewusstsein in der Industrie ist umso verwunderlicher, als der Ausfall einer Maschine oder Anlage viel größere Schäden nach sich ziehen kann als im Büroumfeld. Dem Autor

sind Fälle bekannt, in denen eine massive Überflutung mit Anfragen bei so genannten „Denial-of-Service“-Attacken Steuerungsrechner oder Roboter lahm gelegt haben. Dadurch wurden teilweise ganze Produktionslinien gestört. Geldautomaten haben durch die Infektion mit Würmern über das Intranet der Bank ihren Dienst versagt; die Notabschaltung eines Kraftwerks wurde durch die Verwendung eines Büro-Virenschutzes auf einem für die Steuerung sensibler Abläufe eingesetzten Industrie-PC blockiert. In der vernetzten Bürowelt haben derlei Vorfälle und Angriffe auf die Verfügbarkeit zwar in der Regel auch ärgerliche, aber nicht immer derart fatale Auswirkungen. Statt der bisherigen Insellösungen werden zunehmend auch bei industriellen Anwendungen offene Kommunikationsstandards genutzt und eine Anbindung an das Internet vorgenommen. Beides hilft, Daten in Echtzeit auszutauschen und verschiedenste Systeme miteinander zu verknüpfen. Neben den Standardprotokollen verbreitet

Über unseren Autor:

Olaf Siemens ist Vorstand der Innominat Security Technologies AG, Spezialist für Security Appliances im Umfeld industrieller Kommunikation (M2M) und zur Absicherung einzelner IT Systeme. Kontakt: contact@innominate.com

sich auch Microsofts Betriebssystem Windows in Embedded Systemen. Dies erhöht die Notwendigkeit für grundlegende Sicherheitslösungen, da Windows-basierte Systeme – auch in Fertigungsanlagen – besonders gefährdet sind.

Allerdings sind Lösungen, die in der Regel aus der Bürokommunikation stammen, nur begrenzt für industrielle Anwendungen tauglich. Da Sicherheit bis zum Endgerät gewährleistet sein muss, reicht eine zentrale Firewall zum Schutz des Übergangs zwischen Büro- und Industriernetz nicht aus. Firewall-Systeme, die speziell für den Einsatz im industriellen Umfeld konzipiert wurden, unterscheiden sich dadurch von Büroprodukten, dass sie sich beispielsweise für einen breiteren Temperaturbereich eignen, eine hohe Lebensdauer und Robustheit aufweisen, besonders tolerant gegenüber Überspannungen und einfach zu bedienen sind. ✓

Nachlässige Manager an öffentlichen PC

Bei einer Untersuchung in VIP-Lounges mit öffentlich zugänglichen Computer- und Internetzugang auf internationalen Flughäfen hat das IT-Sicherheitsunternehmen Scanit festgestellt, dass es dort von sensiblen Dokumenten, E-Mails und anderen Firmendaten geradezu wimmelte. Top-Manager wären sich des Sicherheitsrisikos außerhalb ihres Unternehmens offenbar nicht bewusst sind und würden so agieren, als ob sie ihren eigenen PC benützen würden. Vor allem E-Mails würden in den Postausgängen der vorinstallierten Programme vergessen und sogar am Desktop „landen“, wo sie von jedem eingesehen werden können. Ein klassischer Fehler sei auch das normale Löschen eines Dokuments, da es von nachfolgenden Benutzern im Normalfall problemlos aus dem Computer-Papierkorb wiederhergestellt werden könne. Außerdem würden festgestellte Virenprobleme dazu beitragen, dass das Ausspionieren und Weiterleiten sensibler Passwörter keine Seltenheit ist. Nach weiteren Untersuchungen war in Internet-Cafes oder Hotels ein vergleichbares Benutzerverhalten zu beobachten. cs

Unterschiedliche Anforderungen an IT-Sicherheit in Büro und Industrie

| | Büro | Industrie |
|--------------------------|--|---|
| Zuverlässigkeit | gelegentliche Fehler tolerierbar „Beta Test“ im Feld üblich | Unterbrechungen nicht hinnehmbar ausgiebige Qualitätssicherung vorausgesetzt |
| Risiko | Verlust von Daten | Verluste bei Produktion, Anlagen oder möglicherweise Gesundheit und Leben |
| Performanz | hoher Durchsatz lange Laufzeiten im Netz akzeptabel | geringerer Durchsatz hinnehmbar lange Laufzeiten kritisch |
| Wideranlauf | lange Zeiten für Wiederherstellung / | anlauf akzeptabel schneller Wideranlauf / Austausch essentiell |
| Risiko Management | Wideranlauf durch Reboot Safety spielt keine Rolle | Hohe Fehlertoleranz erforderlich |
| Homogenität | in der Regel homogenes Umfeld (Betriebssystem etc.) | sehr heterogen |