

Ausgabe #1: Angriff auf die Leitwarte

martin.weimer@dvide-it.de | 28. Oktober 2011

Die Abschottung der IT-Infrastruktur in der Produktion weicht zunehmend auf; netzwerkseitige Anbindungen an die Betriebsleit- und Unternehmensebene werden Alltag. Der unbefugte Durchgriff auf physikalische Anlagen erleichtert sich für Hacker dadurch immens. Eine Eins-zu-eins-Übertragung von Sicherheitskonzepten für Unternehmensnetzwerke greift zu kurz – neue Ansätze sind notwendig.

Spätestens seit W32.Stuxnet ist der Öffentlichkeit bewusst, dass sich gezielte Angriffe nicht auf Firmennetzwerke oder den privaten Rechner beschränken. Aktuell wird der Ableger W32.Duqu in Form eines Remote access-Trojaners in den Medien diskutiert.¹ Der Computerwurm Stuxnet selbst ist in mehrerer Hinsicht bezeichnend: Sein Ziel sind Industrierechner im Produktionsumfeld und damit letztlich technische Anlagen. Diese Anlagen werden in der Regel über eine hierarchische Prozessleit- und Steuerungstechnik bedient. Die Ebenen umfassen Elemente der Visualisierung, der Prozess- und Anlagensteuerung und der Feldteilnehmer wie Prozesssensoren und -aktoren. Im Falle von Stuxnet wurden bis dato unbekannte Windows-Sicherheitslücken und gestohlene digitale Signaturen ausgenutzt. Die Infektion verläuft über einen speziellen Programmierclient, im Krankheitsverlauf wird die Steuerungssoftware manipuliert, und falsche Anweisungen werden für den Anlagenfahrer verschleiert an Antriebssteuerungen übermittelt.² Stuxnet ist jedoch nicht die einzige Bedrohung für technische Steuerungseinrichtungen, auch ist das von Stuxnet angegriffene System nicht das einzige betroffene Ziel. So melden Einrichtungen wie das „Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)“³ nahezu wöchentlich Sicherheitslücken in diverser Steuerungssoftware für Industrieanlagen.



Zentralwarte Klärwerk Hamburg mit Großbildprojektionswand.
Quelle: Fa. KH-Automation Projects GmbH, Fuldaabrück.

100 Bugs in 100 Days

Einen aktuellen, bemerkenswerten Nachweis⁴ dieser Problematik lieferten Ende September 2011 zwei US-Forscher in Zusammenarbeit mit dem ICS-CERT. In einer knapp drei monatigen Untersuchung gelang es ihnen, unzählige Schwachstellen in SCADA-Systemen (Supervisory Control and Data Acquisition) zu identifizieren und über 600 unterscheidbare Softwareabstürze herbeizuführen. SCADA-Systeme dienen unter anderem als Mensch-Maschinen-Schnittstelle zwischen Bediener und eigentlicher Prozesssteuerung; sie sind damit wichtiger Bestandteil und gleichzeitig Angriffspunkt der betrieblichen Prozessleit- und Steuerungstechnik.

¹ www.symantec.com/connect/w32_duqu_precursor_next_stuxnet

² www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

³ www.us-cert.gov/control_systems/ics-cert/

⁴ www.youtube.com/watch?v=29S_Beg71dA&feature=player_embedded

Bewährte Empfehlungen in neuem Umfeld

Grundlegende Sicherheitshinweise an die Anlagenbetreiber – auch mit Blickrichtung auf obige Problematik unzureichend sicherer Software – sind jedoch nur bedingt an die potentiellen Bedrohungsszenarien angepasst⁵: So sind Betreiber angehalten, eine größtmögliche Abschottung und Absicherung der Steuerungseinrichtungen in Bezug auf deren Netzanbindung vorzunehmen und ein robustes Patch-Management zu etablieren. Diese Maßnahmen entsprechen nicht dem allgemeinen Trend. Proprietäre, physikalische und netztechnisch isolierte Systeme wandeln sich zu dokumentierten, standardisierten und angebotenen Systemen. Es erfolgt eine zunehmende innerbetriebliche vertikale Integration der Systeme, eine Ablösung proprietärer Bussysteme und die Bereitstellung von Wartungsmöglichkeiten von außen. Zugriffe über mobile Apps auf SCADA-Systeme stellen derzeit die Speerspitze einer betrieblichen Durchlässigkeit dar. Auch kann oftmals ein wirkungsvolles Patch-Management nicht umgesetzt werden, wenn zu viel Zeit zwischen Erkennen einer Schwachstelle und Freigabe bzw. der Bereitstellung von Hotfixes und Security Patches verstreicht oder weil kaum Wartungsfenster im betrieblichen Ablauf vorgesehen sind.

Bedarf an neuen Lösungen

Daher besteht jenseits dieser Empfehlungen die Notwendigkeit für unterschiedliche Entwicklungsaufgaben für die bayerische Automatisierungsindustrie und Anbieter von IT-Sicherheitslösungen. Einige seien exemplarisch ohne Hinweis auf Priorität genannt:

- ▶ Methoden und Werkzeuge zur Operationalisierung von Sicherheitsstandards im Bereich Prozessleitsystem / Mensch-Maschine-Schnittstelle / SCADA
- ▶ Sichere Kommunikationsprotokolle der Leitebene, Steuerungs- und Feldebene

- ▶ Firewalling für Leitstände unter Berücksichtigung der Echtzeitanforderungen
- ▶ Neue Authentifizierungsverfahren und Autorisierungsmodelle im Umfeld von Leitständen insbesondere rollenbasierte Zugriffe oder sichere Webservices
- ▶ Lösungen für die hochsichere Fernwartung von Produktionsanlagen
- ▶ Lösungen zur sicheren Netzwerk-Segmentierung

Dem Schutz von Leitsystemen wird in Zukunft eine noch größere Bedeutung beigemessen. Dies verwundert angesichts der zunehmenden Vernetzung im Energiebereich nicht. Jede Domäne dieses Bereichs – sei es die Erzeugung von Energie, deren Übertragung oder Verteilung – wird durch Leitsysteme gesteuert. In einem Smart Grid sind alle Leitsysteme einer übergeordneten Steuerung über WAN oder das Internet miteinander verbunden. Die Angriffsmöglichkeiten sind daher ungleich größer als in konventionellen Energiekonzepten.

Das Bayerische Wirtschaftsministerium fördert innovative Verbundprojekte auch zum Thema „Rechnernetze“ im Rahmen des Programms Informations- und Kommunikationstechnik Bayern www.iuk-bayern.de. Sollten Sie Projektvorschläge haben, kontaktieren Sie uns bitte.

⁵ www.bsi.bund.de/ContentBSI/Themen/Kritis/Einfuehrung/Empfehlungen/empfehlungen.html