

30.09.08

Von: Thomas Gronenwald, Florian Thiessenhusen

## **adMERITia: SCADA-Systeme kommen in sogenannten Prozessdatennetzen (PDN), Prozessnetzen (PZN) oder Prozesssteuerungsnetzen (PSN) zum Einsatz.**

### **SCADA - Sicherheit im Produktionsumfeld**

Automatisierungs- und Prozesssteuerungssysteme werden weltweit in nahezu allen Industrieunternehmen eingesetzt. Der Trend und die Entwicklung gehen dabei weg von proprietären und isolierten Feldbussystemen hin zu standardisierten und gekoppelten Netzwerken.

Welche Sicherheitsrisiken bergen solche Entwicklungen in der Automatisierungs- und Prozesssteuerungstechnik innerhalb von kritischen Infrastrukturen und wie kann wirkungsvoll entgegengewirkt werden? Dieser Artikel beschreibt die Risiken und Maßnahmen zur Minimierung solcher hochkritischen Prozesssteuerungen.

### **Was ist SCADA?**

Das Akronym SCADA steht für "Supervisory Control and Data Acquisition" und ist ein Synonym für die Echtzeit-Überwachung, Steuerung und Datenerfassung von technischen Prozessen innerhalb von industriellen Automatisierungsanlagen. Vereinfacht ist SCADA der Punkt im Automatisierungsumfeld, der überwacht und entscheidet, "was zu tun ist", "wenn etwas passiert". Im Automatisierungsumfeld wird diese Entscheidung als "event driven" bezeichnet. Heutzutage sind solche Systeme nicht mehr aus den Produktionsdatennetzen der großen und mittelständigen Industrieunternehmen wegzudenken. Dabei siedeln sich viele dieser Systeme innerhalb von so genannten kritischen Infrastrukturen (engl. Critical Infrastructure Protection - CIP) an.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert kritische Infrastrukturen dabei wie folgt: „Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachteilig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“ („Bundesamt in der Informationstechnik“, <http://www.bsi.bund.de/fachthem/kritis/definitionen.htm>, 29.09.2008)

### **Zu den kritischen Infrastrukturen gemäß KRITIS werden gezählt:**

- Transport und Verkehr,
- Energie (Elektrizität, Öl und Gas)
- Gefahrenstoffe (Chemie und Biostoffe, Gefahrguttransporte, Rüstungsindustrie)

- Informationstechnik und Telekommunikation
- Finanz-, Geld- und Versicherungswesen
- Versorgung (Gesundheits-, Notfall- und Rettungswesen, Katastrophenschutz, Lebensmittel- und Wasserversorgung, Entsorgung)
- Behörden, Verwaltung und Justiz (einschließlich Polizei, Zoll und Streitkräfte)
- Sonstiges (Medien, Großforschungseinrichtungen sowie herausragende oder symbolträchtige Bauwerke, Kulturgut).

SCADA-Systeme kommen dabei in sogenannten Prozessdatennetzen (PDN), Prozessnetzen (PZN) oder Prozesssteuerungsnetzen (PSN) zum Einsatz. Eine Standardisierung der Begrifflichkeiten für produktionsnahe Systeme gibt es hierbei jedoch nicht. Im generellen spricht man bei solchen Netzen von "Industrial Ethernets".

## **Sicherheitsrisiko SCADA**

Nicht zuletzt durch die vielen, in kürzerer Vergangenheit, aufgetauchten Schwachstellen in den Anlagen führender Industrieunternehmen, rückt das Thema "Sicherheit" auch in solchen Strukturen mehr und mehr in den Fokus von Verantwortlichen, Betreibern und Sicherheitsexperten.

Einer der bedeutendsten Vorfälle war hier wohl der größte Stromausfall in der Geschichte der USA/Kanada im Jahr 2003, hervorgerufen durch den allseits bekannten Wurm W32.Blaster. Dieser konnte sich, unterstützt durch fehlende Sicherheitsmaßnahmen, bis in die Kraftwerkssteuerungen einschleusen und sich von dort aus weiterverbreiten. Aber nicht nur durch eingeschleuste Malware und Viren sind solche Systeme gefährdet, auch durch immer wieder veröffentlichte Exploits werden IT-basierte Systeme immer stärker angreifbar. Da in diesen Fällen zumeist kein oder nur ein begrenztes Patchmanagement betrieben wird, sind solche Systeme über mehrere hundert Exploits und kritische Sicherheitslücken angreifbar. Hinzu kommt, dass SCADA-Systeme zumeist eine deutlich längere Lebens- bzw. Nutzungsdauer als normale Bürosysteme besitzen. Hier ist es durchaus normal, dass SCADA-Systeme fünf oder mehr Jahre im Dauereinsatz sind. Im Vergleich dazu sind Bürosysteme meist nur mit einer durchschnittlichen Nutzungsdauer von drei Jahren in Betrieb. In Kombination mit dem Sicherheitsziel der Hochverfügbarkeit ist es keine Seltenheit, dass solch produktionsnahen Systeme im Laufe ihres Lebenszyklus nicht oder zu wenig im Bereich der IT-Sicherheit gewartet werden. Dies gilt sowohl für den Bereich der organisatorischen, als auch für den Bereich der technischen Sicherheit.

Die Anforderung der Bereitstellung von gesammelten Prozessdaten zu Abrechnungs- oder Überwachungszwecken, bedingt dabei eine Kopplung zum Corporate-LAN (Büronetz), macht eine bestehende Netzwerkverbindung unausweichlich. Das BSI empfiehlt in seinen Maßnahmenkatalogen in solchen Fällen die strikte Trennung der Netze, zumindest durch eine Firewall (Paketfilter). Jedoch ist dies in der Praxis vergleichsweise selten zu finden. Netztrennungen sind nicht vorgesehen oder gar mangelhaft implementiert, ein direkter ungefilterter Zugriff von Corporate-LAN zum SCADA-System ist so zumeist möglich.

Jedoch wird IT-Sicherheit auch in Prozessnetzen nicht nur durch punktuelle Sicherheitskonfigurationen wie etwa durch eine Firewall erreicht. Wesentlich wichtiger ist es, alle Faktoren und Prozesse zu kennen und hier geeignete Sicherheitskonzepte für alle Faktoren zu erstellen und zu implementieren. Hierbei ist es empfehlenswert, Partner und Sicherheitsexperten mit in diese Prozesse einzubinden, sowohl in der Planungs- als auch in der Implementierungsphase. Ein entscheidender und elementarer Punkt ist die Absicherung des Betriebssystems eines SCADA-Systems. Dabei kommen Unix Systeme immer seltener zum Einsatz. Unter anderem aus Interoperabilitäts-, Funktions- und Kostengründen mit der vorhandenen Netzwerkumgebung, setzen die Hersteller einschlägiger SCADA-Systeme häufiger auf Windowssysteme. Dies hat für den Kunden den Vorteil, dass

Gesamtstrukturfunktionsdienste, wie etwa DNS, WINS oder Verzeichnisdienste, wie Active Directory, weiterhin Windows integriert genutzt werden können. Ob Unix oder Windows, Betriebssystemsicherheit ist für beide Systeme wichtig und kann in 24x7 Umgebungen nicht immer gewährleistet werden.

## Hersteller von SCADA -Systemen

Während ursprünglich in der Prozessleittechnik und Anlagenüberwachung nur sehr spezialisierte und proprietäre Systeme und Anlagen eingesetzt wurden, geht heute der Weg in Richtung offene Standards. Hierbei spielt nicht zuletzt der immer größer werdende Kostendruck eine nicht zu unterschätzende Rolle, sondern auch die Interoperabilität zwischen den Systemen verschiedener Hersteller. Hierbei werden zunehmend die klassischen Feldbussysteme gegen modernere TCP/IP basierende Industrial Ethernets ausgetauscht. Heutzutage liefern Hersteller aus der ganzen Welt SCADA-Applikationen wie etwa GE Fanuc (iFix), Siemens PowerCC und WinCC oder ABB 800xA. Auch geht der Trend in Richtung Windows basierender Applikationen. Da dort in den meisten Szenarien keine Embedded-Versionen zum Einsatz kommen, gibt es hier die gleichen Sicherheitsrisiken wie auf einem vollwertigen, aus der Bürowelt bekannten System.

## Ist eine Absicherung von SCADA überhaupt möglich?

Einer der größten Fehler, der bei der Absicherung von SCADA- Systemen begangen wird, ist der Versuch der Adaptierung von Sicherheitsfunktionen aus Büroumgebungen. Dies erfordert ein Umdenken der verantwortlichen IT sowie den Errichtern von Sicherheitssystemen.

Durch die Komplexität, die eine SCADA-System mit sich bringt, sowie der hohen Anforderung an die Verfügbarkeit, wird weitläufig angenommen, dass eine Absicherung wenig praktikabel ist und den Betrieb stören oder beeinträchtigen könnte. Der größte Trugschluss ist, dass SCADA-Systeme mit einem Tool, Programm oder einer Maßnahme komplett abgesichert werden können. Es ist ein Bündel an organisatorischen und technischen Maßnahmen notwendig, um eine gewisse Sicherheit zu erreichen. Diese werden im Folgenden näher erläutert.

## Absicherungsszenarien

Es reicht nicht aus, punktuelle Sicherheitsmaßnahmen durchzuführen. Alle durchzuführenden Maßnahmen sollten aufeinander abgestimmt sein und in der Konsequenz eine einheitliche Sicherheitsbasis bilden.

Folgende Themenkomplexe (die im Weiteren näher beschrieben werden) sollten bei der IT-Sicherheit von SCADA-Systemen berücksichtigt werden:

- Organisatorische Sicherheit
  - Security-Awareness
  - Security Policies
  - Sicherheitsanalyse und Risikoanalyse
  - Prozesssicherheit
  
- Technische Sicherheit
  - Segmentierung in DCN (Distributed Control Network), PCN (Process Control Network) und PIN (Process Information Network)
  - Firewall, Segmentierung (DMZ)
  - Virenschutz

- Zertifizierung der Lösung durch SCADA-Hersteller
- Backup-Konzepte
- Hardening (TCP/IP), Service Account Hardening
- Passwörter
- Verzeichnisdienstsicherheit

## **Organisatorische Maßnahmen zum Schutz von SCADA -Systemen**

Die Sicherheit muss von allen Beteiligten im Automatisierungs- und Produktionsumfeld gelebt werden, damit sie effektiv sein kann. Virens Scanner schützen nur, wenn sie aktiv sind; Firewalls sind nur sinnvoll, wenn sie auch scharf geschaltet werden. Sicherheit muss also in den Köpfen aller Mitarbeiter und selbstverständlich auch in den Köpfen der Betriebsverantwortlichen fest verankert sein.

Um diese Ziele zu erreichen, sollte Sicherheit klar, nachvollziehbar und vor allem transparent für jeden sein. Schließlich geht es darum, einen kostspieligen Produktionsprozess abzusichern. Nur wenn klare Strukturen, Richtlinien und Guidelines bestehen, kann Sicherheit von jedem Mitarbeiter gelebt und umgesetzt werden.

### **Sicherheitsrichtlinie**

Sicherheitsrichtlinien für Automatisierungs- und Produktionsumfelder sind nicht vergleichbar mit Sicherheitsrichtlinien für herkömmliche IT-Systeme. Hierbei spielen viele entscheidende Faktoren eine große Rolle, die in einer herkömmlichen Richtlinie nur selten tangiert werden. Eine solche Sicherheitsrichtlinie kann nicht einfach adaptiert werden, sondern muss auf die entsprechenden Prozesse und Steuerungen angepasst werden. Hierzu haben sich in der Vergangenheit einige Leitfäden und ISO-Normen als Grundlagen herauskristallisiert. Darunter die ISO 27001 und 27002 als auch die Beispielrichtlinie "IT-Sicherheit im KRITIS-Unternehmen - Ein Beispiel aus der Praxis" des BSI. Die Entwicklung und Umsetzung eines solchen IT-Sicherheitskonzeptes für SCADA- und Automatisierungsumgebungen, sowie die Etablierung ist ein höchst anspruchsvolles und arbeitsintensives Projekt, welches nicht unterschätzt werden sollte. Insbesondere in der Planungsphase kann die Unterstützung durch einen kompetenten Partner oder Berater sehr hilfreich sein. Außerdem beweist es sich als sinnvoll, in regelmäßigen Abständen Security Audits durchzuführen, um so bereits Risiken und Schwachstellen zu beseitigen. Das Open Source Security Testing Methodology Manual (OSSTMM) der Herausgeberin ISECOM (Institute for Security and Open Methodologies) bietet hierfür geeignete Sicherheitstestschritte und beschreibt eine Methode, wie technische Security Audits geplant, durchgeführt und dokumentiert werden sollten.

### **Segmentierung**

Die wichtigste Maßnahme bei der Absicherung von Netzwerken ist das Aufteilen von Netzsegmenten, unter Zuhilfenahme von Firewalls, die den Verkehr dazwischen filtern.



direkter Zugriff aus dem Corporate-LAN ins das DCN kann nicht erfolgen.

Zudem ist das DCN durch zwei Firewalls vom PCN getrennt. Die Besonderheit dabei ist, dass zu den Aktoren häufig proprietäre Protokolle zum Einsatz kommen und dies bei der Beschaffung und Implementierung der Firewall berücksichtigt werden muss.

## Virenschutz

In Bereich von Windowsumgebungen ist Virenschutz ein sehr wichtiges Thema. Gerade bei nicht ausreichend getrennt aufgebauten Netzwerken (fehlende Trennung Corporate Net von SCADA Netzwerk) ist möglich, dass schadhafter Code bis zu den, vermeintlich ungeschützten, SCADA Systemen gelangt.

Ein gängiger Virenschutz hat sich auf windowsbasierten SCADA- Systemen bisher nicht durchgesetzt. Dies ist darin begründet, dass Hersteller von SCADA's nicht immer Aussagen darüber treffen können, ob ein Virenschutz das Prozessleitsystem negativ beeinflussen kann. Ein selbst installierter Virenschutz würde im schlimmsten Fall einen Garantieverlust des Systems nach sich ziehen.

In seltenen Fällen kann jedoch bei den Herstellern von SCADA-Systemen eine selbst zertifizierte und getestete Lösung erworben werden. Wenn jedoch eine Sicherheitsrichtlinie vorschreibt, dass nur ein spezieller Virenschutz im Unternehmen zu nutzen ist (und somit den Einsatz einer differierenden Lösung des Herstellers untersagt), dann sollte der eigene Virenschutz beim Hersteller zertifiziert werden. Dabei werden folgende Aspekte getestet:

- Anteil der Systemlast des Echtzeitschutzes
- Ordner- und Dateiausnahmen
- Lauffähigkeit des Gesamtsystems im Dauertest
- Systemverhalten bei Signaturupdates
- Verhalten bei Virusfund

Nach erfolgreicher Zertifizierung kann die eigene Virenschutzlösung auf dem entsprechenden SCADA-System ausgerollt werden.

## Backup

Für Systeme, die eine Verfügbarkeitsanforderung von 24x7 haben, muss eine schnelle Wiederherstellung gewährleistet sein. Ein Backupsystem muss dafür implementiert werden. Es kann zwischen verschiedenen Lösungen gewählt werden:

## Imaging

Hierbei wird ein System im Imaging-Verfahren gesichert. Dies ist die wahrscheinlich sicherste Methode, um im Disasterfalle ein komplettes System wiederherzustellen. Jedoch nimmt ein Sicherungsvorgang sehr viele Systemressourcen ein und es muss getestet werden, wie sich dies auf die Prozesskette auswirkt. Mehrere Produkte sollten evaluiert werden, um ein geeignetes zu finden.

SCADA-Systeme sind häufig mit spezieller Hardware ausgestattet. Bei der Wiederherstellung wird eine sogenannte Wiederherstellungsumgebung genutzt. Diese muss mindestens Festplatten-Controller (sofern vorhanden) erkennen und auf die Festplatten schreiben können. Es stellt sich meistens als schwieriges Unterfangen heraus, geeignete Treiber für speziell verbaute Hardware zu finden.

## **Dateisicherung**

Eine Alternative zum Imaging-Verfahren stellt die Dateisicherung nur bedingt dar. Eine Wiederherstellung im Desaster-Fall ist Zeitaufwendig (das Betriebssystem sowie die Applikationen müssen mindestens manuell installiert werden). Jedoch hat man mit der normalen Dateisicherung eher die Möglichkeit, Voll- und Zuwachssicherungen in engen Abständen durchzuführen.

Es sollte je nach Verfügbarkeitsanforderung und definierter Wiederanlaufzeit eines Servers entschieden werden, welche Sicherungsmethode zum Einsatz kommt.

## **Hardening**

Denial of Service Attacken (DoS), angewendet auf Produktionssysteme, sind weit verbreitet und bekannt. Hierbei wird das Produktionssystem solange mit bestimmten Anfragen penetriert, bis das System seine Arbeit einstellt. Ziel des TCP/IP Hardening ist es, Maßnahmen zu treffen, welche diese Angriffe erschweren oder gar vermeiden. Beispielsweise können mit dem Parameter "SynAttackProtect" innerhalb des TCP/IP Stacks bereits erste Maßnahmen getroffen werden, um solchen Gefahren aus dem Weg zu gehen.

## **Passwörter**

Viele Hersteller von SCADA-Systemen nutzen für Ihre Kunden Standardpasswörter, die auch nach Produktivschaltung nicht geändert werden. Dies gilt auch für die Anwender. In solchen Umgebungen wird häufig mit Funktions-Accounts gearbeitet, die gleichzeitig Administratoren sind.

Eine Passwortrichtlinie mit diversen Ausprägungen und bestimmten Changeintervallen, wie man sie häufig in Corporate-Netzwerken findet, ist für solch ein Produktionsnetz nicht praktikabel. Trotzdem sollte eine speziell auf die Produktionsbedürfnisse angepasste Richtlinie implementiert werden. Selbst wenn die Passwörter nicht komplex sind, so stellt ein regelmäßiger Passwortwechsel für Angreifer (oder ausgeschiedenen Mitarbeitern) immer ein höheres Hindernis dar.

## **Verschlüsselungen**

Um Applikationen auf den Server zu verlagern und den Benutzern einen einfachen Zugriff auf die Daten zu gewährleisten, werden immer mehr SCADA Applikationen auf Webanwendungen verlagert (eher Datenauswertung). Die Gefahr, dass dort sensible Daten ausgespäht werden können ist enorm hoch, daher sollte der Verkehr abgesichert werden, zum Beispiel mit SSL.

Verschlüsselung ist ebenfalls ein Thema bei der Absicherung von Netzwerkprotokollen die nicht über eine eigene Verschlüsselungsmöglichkeit verfügen. In diesem Falle kann man sich der Verschlüsselung über einen sicheren IPsec Tunnel bedienen. Verkehr, der nicht verschlüsselt ist, wird nicht zugelassen.

## **Patchmanagement-Strategien**

Patchmanagement ist eine der wichtigen Aufgaben von Verantwortlichen und Betreibern zum Schutz vor Sicherheitslücken innerhalb der Produktionsumgebungen. Durch nicht behobene Sicherheitslücken ist es beispielsweise möglich, Zugriffe auf Systeme zu erlangen oder mithilfe von Brute-Force-Angriffen oder Exploits ein System komplett zu übernehmen. Da es zumeist innerhalb von Produktionsnetzen keinerlei solcher Strategien oder Methoden gibt, sind die Systeme äußerst anfällig. Durch einen 24x7 Betrieb ist es auch alles andere als einfach, dort geeignete Konzepte zu implementieren und zu nutzen. Jedoch gibt es einige probate Ansätze

die es ermöglichen, solche Systeme auch mit einer Patchmanagement-Lösung zu betreiben. Natürlich müssen dafür auch Disaster-Recovery-Pläne, sowie Backup-Strategien entwickelt werden, um im Notfall betroffene Systeme wieder herstellen zu können. Redundanz spielt in solchen Konstellationen eine große Rolle und ist heutzutage durchaus im Rahmen des möglichen.

## **Verzeichnisdienstabsicherung**

Zur Authentifizierung der Benutzer innerhalb von Produktionsdatennetzen, werden zumeist Verzeichnisdienste wie beispielsweise das Active Directory von Microsoft eingesetzt. Hier gibt es umfangreiche Möglichkeiten, zentralisiert über Gruppenrichtlinien, eine Sicherheit für alle Microsoft-basierten Systeme zu schaffen. Anhand verschiedener Rollen können dort Härtingsmaßnahmen getroffen und die Sicherheit signifikant erhöht werden.

Fazit: SCADA Absicherung ist möglich!

*Autor:*

*Thomas Gronenwald, Security Consultant  
Florian Thiessenhusen, Security Consultant*

**adMERITia GmbH**

**Gladbacher Straße 3**

**40764 Langenfeld**

**Tel. +49 (2173) 20363-0**

**Fax +49 (2173) 20363-29**

**<http://www.admeritia.de>**

- Verwandte Themen
- adMERITia: UPnP bietet Angreifern eine Vielzahl an Möglichkeiten ein System zu manipulieren
- adMERITia GmbH: Man kann nicht managen, was man nicht misst!

**Copyright All-About-Security.de / [www.all-about-security.de](http://www.all-about-security.de) Alle Rechte vorbehalten**  
Vervielfältigung nur mit Genehmigung von All-About-Security.de