

newsletter

zum Thema **Stuxnet & Co**

IT-spezifische Gefährdungen für industrielle Prozesssteuerungen

Bisher war Schadsoftware (Malware) hauptsächlich im PC-, Office- und Internetbereich anzutreffen, um beispielsweise Zugangsdaten (z.B. Username und Passwörter) auszuspionieren. In 2010 tauchte mit dem Trojaner Stuxnet erstmalig eine Malware auf, die gezielt für Angriffe auf industrielle Prozesssteuerungen entwickelt wurde. Kürzlich wurde von IT-Experten erneut eine Schadsoftware (Duqu) entdeckt, die Unternehmen, welche sich mit der Entwicklung von Industrieanlagen befassen, ausspionieren sollte. Diese Beispiele zeigen, dass Attacken auf Prozesssteuerungssysteme mittels Malware in zunehmendem Maße ein Gefährdungspotential darstellen, das es zukünftig bei Risikobewältigung und -bewertung zu berücksichtigen gilt.

**Auto-
matisierungs-
und Prozess-
steuerung-
systeme**

Die zur Steuerung, Monitoring und Kontrolle bei Industrieanlagen eingesetzten IT-Systeme werden unter dem Oberbegriff Prozesssteuerungs- oder MSR-Systeme (Messen, Steuern, Regeln) zusammengefasst. Im Englischen spricht man von DCS (Distributed Control Systems) und SCADA (Supervisory Control and Data Acquisition) Systemen. Charakteristisch für derartige Systeme ist ihr modularer Aufbau aus einzelnen Komponenten. Beispielhaft seien hier Speicherprogrammierbare Steuerungen SPS (englisch Programmable Logic Controller PLC), die für die elektronische Steuerung und Regelung von Maschinen oder definierten Prozessteilen eingesetzt werden, genannt. Prozesssteuerungs- und -leitsysteme (MSR/SCADA-Systeme) kommen in praktisch allen Prozessinfrastrukturen zum Einsatz, die physische Prozesse kontrollieren – von der Anlagensteuerung in Raffinerien über die Energieerzeugung und -verteilung bis hin zur Verkehrsleittechnik und Güterherstellung in der industriellen Produktion.

**Zunehmende
Standardisierung
und Vernetzung**

In den letzten Jahren hat sich die moderne Informationstechnologie zunehmend in den Bereich der klassischen Prozesssteuerungs- und Automatisierungstechnik ausgebreitet. Die industrielle Steuerungstechnik zeichnete sich bislang durch IT-Systeme aus, die untereinander mit eigenen, u.a. nicht mit anderen Systemen kompatiblen Protokollen und Techniken kommunizieren sowie meist auf proprietären Softwarelösungen basieren. In der Vergangenheit waren sie dadurch vom Großteil der in der klassischen Datenverarbeitung und Bürokommunikation eingesetzten Informationstechnologie autonom und separiert.

Mittlerweile breitet sich auch in diesen Umgebungen die sonst allgegenwärtige Netzwerktechnik auf Basis von Ethernet und TCP/IP sowie Standardsoftware in zunehmendem Maße aus. Das Spektrum erstreckt sich hier auf den Einsatz von Standardsoftware wie Datenbanken über Standard-Hardware, die mit Windows oder Unix basierenden Betriebssystemen ausgestattet ist. Mit diesem Zusammenwachsen können vermehrt Synergien genutzt werden, und es ermöglicht Standardisierung, Flexibilisierung und verbesserten Datenaustausch. Insbesondere die Auswertbarkeit und Visualisierung von Prozessdaten für ein zentralisiertes Management sowie die zu erzielenden Kosteneinsparungen bei der Entwicklung und Anschaffung der Systeme werden in diesem Zusammenhang als Hauptvorteil gesehen.

Grundsätzlich ist die Sicherheit im industriellen Prozessumfeld in vielen Bereichen weit entwickelt, bezieht sich aber vorwiegend auf Themen wie Ausfallsicherheit, Explosionsschutz, Arbeitssicherheit oder elektrische Sicherheit.

Sicherheitsrisiken wie Computerviren, Denial of Service- oder Hackerattacken, die in der klassischen Datenverarbeitung und Bürokommunikation eingesetzten Informationstechnologie seit langem zum Alltag gehören, wurden in diesem Umfeld in der Vergangenheit weit weniger Beachtung geschenkt.

Stuxnet

„Stuxnet“ ist der Name für eine Malware, die im Sommer 2010 entdeckt wurde. Stuxnet fand weit über Fachkreise hinaus auch in der breiten Öffentlichkeit Beachtung, da er wegen seiner Komplexität und des Angriffsziels einen Paradigmenwechsel im Bereich der Schadsoftware darstellte. Stuxnet wurde gezielt programmiert, um Industrieanlagen zu sabotieren. Das Programm hatte das Ziel, ein bestimmtes System der Firma Siemens, das zur Steuerung und Überwachung technischer Prozesse eingesetzt wird, umzuprogrammieren. Dabei wurde vor allem die Steuerungssoftware WinCC (Windows Control Center) und das Prozessleitsystem SIMATIC PCS 7 von der Malware in den Fokus genommen. Stuxnet nutzt für seinen Infektionsprozess gleichzeitig mehrere zum Zeitpunkt seines Auftretens unbekannte Windows-Schwachstellen (Zero-Day-Exploits) sowie gestohlene Signaturen von namhaften Hardware-Herstellern.

Der erste Verbreitungsschritt erfolgt über ein Wechselmedium wie z.B. einen USB-Stick. Nachdem das Schadprogramm im Zielsystem eingedrungen ist, versucht es sich im System zu tarnen und kann sich dann über verschiedene Möglichkeiten über Netzwerke verbreiten. Stuxnet kann in den infizierten Steuersystemen Code ändern, so dass von den Betreibern unbemerkt Dritte die Kontrolle über ihre Systeme erlangen können.

Befallen wurden Industrieanlagen auf der ganzen Welt, wobei die meisten Stuxnet-Infektionen in Indien, Indonesien und im Iran auftraten. Die Atomanlagen des Iran wurden als vermeintliches Hauptziel der Stuxnet-Attacke identifiziert. In den entsprechenden Rechnern der iranischen Atomaufbereitungsanlagen soll Stuxnet über die Steuerungssysteme die zur Urananreicherung benutzten Zentrifugen manipuliert und in Folge auch den Anreicherungsprozess beeinträchtigt haben. Sicherheitsexperten bescheinigen Stuxnet eine bis dato unbekannte technische Ausgereiftheit und hohe Komplexität. Seine Entwicklung hat ein hohes Maß an spezifischen Fachkenntnissen sowie entsprechend große personelle und finanzielle Ressourcen erfordert.

Duqu

Im Oktober 2011 wurde eine Schadsoftware entdeckt, die gezielt auf Unternehmen gerichtet war, welche im Bereich der Entwicklung von Industrieanlagen tätig sind. Diese neue Schadsoftware mit dem Namen Duqu, ist ein Trojaner, der ganz spezifisch Daten von den Herstellern industrieller Kontrollsysteme sammelt, um diese dann an die Malware-Entwickler zu übermitteln.

Da Duqu zumindest in Teilen auf dem Software-Code von Stuxnet basieren soll, wurde er in Expertenkreisen auch als dessen „kleiner Bruder“ betitelt. Es wird vermutet, dass die durch den Trojaner gewonnenen Informationen für zukünftige Attacken auf Industrieanlagen genutzt werden können.

Hinweise für das Underwriting

Die Attacke von Stuxnet hat aufgezeigt, dass Angriffsversuche auf kritische Infrastrukturen und deren industrielle Prozesssteuerungen nicht nur theoretisch denkbar, sondern durchaus jetzt bereits möglich sind und in Zukunft wahrscheinlicher werden. Duqu hat unter anderem aufgezeigt, dass Stuxnet spezifisches Know how wie z.B. der Quellcode sich in Hacker-Kreisen bereits weiter verbreitet hat. Bei gleichbleibendem Schutzgrad der Industrieanlagen erhöht das die Wahrscheinlichkeit eines erfolgreichen Angriffes in der Zukunft.

Durch diesen Angriff wurde weltweit der Fokus auf eine Schwachstelle gerichtet, die bis dato nur wenig Beachtung fand – nämlich IT-Sicherheit im Bereich der industriellen Prozesssteuerungen bzw. bei den mit ihnen verbundenen IT-Systemen. Die bestehenden Sicherheitsphilosophien industrieller Prozesssteuerungen sollten diesbezüglich hinterfragt, angepasst und gegebenenfalls aufgerüstet werden um diesen neuen Bedrohungen Rechnung zu tragen. Die Abhängigkeit industrieller Prozesssteuerungen von zunehmend standardisierten und vernetzten Informationstechnologien wird weiter zunehmen.

Cyber-Attacken auf industrielle Prozesssteuerungen können - indem Prozesse und Anlagen manipuliert werden - beispielsweise zu Feuer- und Explosionsereignissen und in Folge zu Betriebsunterbrechungen führen. Versicherungsseitig können derartige Angriffe hauptsächlich Property-, Maschinenbruch-, und Betriebsunterbrechungsdeckungen (BI/CBI) sowie haftpflichtseitig Betriebs- und Umwelthaftpflichtpolice betreffen und da zu versicherten Schadenereignissen führen.

Aufgrund des Verbreitungsgrads der Systeme und deren Netzanbindung besteht auch ein signifikantes Kumulschadenpotential.

Kontakt

AssTech GmbH
Postfach 1211
85766 Unterföhring bei München
Telefon + 49 89 3844-1585
Telefax + 49 89 3844-1586
info@asstech.com
www.asstech.com