FOKUS: NETZWERKE

Industriekontroll-systeme ausser Kontrolle

Computersysteme zur Kontrolle von Industrieanlagen sind meist ungenügend gesichert. Wie Unternehmen ihre Anlagen schon mit geringem Aufwand effektiver schützen können, zeigt der folgende Beitrag.

BILD: ISTOCKPHOTO.COM/LEUNGCHOPAN

→ **VON MICHAEL ASSANTE**

Nur selten dringen Nachrichten über Angriffe auf Industriekontrollsysteme an die Öffentlichkeit. Die Attacke auf das iranische Atomprogramm mithilfe des Wurms Stuxnet war lange Zeit der einzige schwerwiegende Fall, der in breiten Kreisen bekannt wurde. Einen weiteren Vorfall hat kürzlich das deutsche Bundesamt für Sicherheit und Informationstechnik (BSI) in seinem Jahresreport veröffentlicht. Das Industry Control System (ICS) eines deutschen Stahlwerks ist 2013 Opfer eines sogenannten Cyber-to-Physical- bzw. Process-Effects-Angriffs geworden. Erhebliche physische Schäden an Teilen der Anlage waren die Folge.

Dass nicht mehr solcher Fälle bekannt sind, liegt daran, dass sie oft nicht gemeldet werden. Zwar gibt es staatliche und private Meldestellen, die auch anonymisierte Informationen über Cyberangriffe annehmen, doch wird diese Möglichkeit immer noch viel zu selten genutzt. Grössere, börsennotierte Unternehmen fürchten um eine Senkung ihres Aktienwerts, sollte die Verletzlichkeit ihrer Produktionsanlagen bekannt werden. Bislang sind es vor allem kleinere Unternehmen, die Informationen über Angriffe zur Verfügung stellen.

Michael Assante ist Projektleiter für ICS und Supervisory Control and Data Acquisition (SCADA) Security beim SANS Institut → **www.sans.org**

EIN STAHLWERK ALS ANGRIFFSZIEL

Zu Beginn der Attacke auf das deutsche Stahlwerk wendeten die Kriminellen Spear-Phishing in Kombination mit Social Engineering an. Unter Spear-Phishing versteht man eine ausgefeilte Phishing-Methode, die speziell auf die Gruppe der Opfer zugeschnitten ist – dadurch steigt die Wahrscheinlichkeit, dass diese auf den Betrug hereinfallen. E-Mails wurden an Mitarbeiter des Unternehmens versendet, und zwar primär an solche, die für die Unterhaltung der Produktionsanlagen zuständig waren. Die Identität der Angreifer konnte bislang nicht ermittelt werden, doch ist anzunehmen, dass sie hohe technische Fertigkeiten besassen. Neben Kenntnissen über die IT-Sicherheit des Unternehmens dürften sie auch über solche zu einzelnen ICS und Produktionsprozessen verfügt haben. Das ist bislang alles, was vom BSI aufgedeckt wurde.

Wie Hacker ein Stahlwerk angreifen könnten, zeigen die nachfolgenden Ausführungen. Alles, was nun folgt, ist ein rein hypothetisches Szenario und hat nichts mit dem Vorfall in Deutschland im Jahr 2013 zu tun.

WIE EIN ANGRIFF ABLAUFEN KÖNNTE

Mails mit kompromittierten Anhängen werden oft genutzt, um einen Fuss in die Tür des Unternehmens zu bekommen. In diesen Mails könnte sich ein PDF mit Malware befinden. Öffnet ein Mitarbeiter das PDF, aktiviert er gleichzeitig, ohne es zu bemerken, die Malware. Fortan können die Angreifer unbemerkt auf die Anwendung zugreifen und sich im Netzwerk des Unternehmens bewegen. Schrittweise können sie sich bis in die ICS der Produktionsanlagen vorarbeiten. Ein Umstand kommt ihnen dabei meist sehr entgegen: ICS sind zwar ursprünglich abgeschottet von den übrigen Netzwerken des Unternehmens angelegt worden, also als digitale Inseln. Die Unternehmen wollen aber nicht zur Gänze auf einen schnellen Zugriff auf ihre Produktion verzichten. So entsteht eine digitale Vernetzung zwischen Unternehmen und Produktionsanlage, zu denen im Rahmen von Optimierungsprozessen weitere Verbindungen treten. Letztlich bedeutet das eine unkoordinierte und schlecht abgesicherte Vernetzung, sodass der Angreifer, hat er erst einmal die internen Systeme des Unternehmens kompromittiert, sich ohne grössere Probleme auch Zugriff auf alle vernetzten industriellen Komponenten verschaffen kann. In unserem hypothetischen Fall liesse sich das ICS eines Hochofens des Stahlwerks, das der Angreifer übernommen hat, schon bald nicht mehr vollständig vom Personal kontrollieren. Einzelne Systemkomponenten des ICS würden ausfallen. Erhebliche physische Schäden am Hochofen und damit auch am Personal wären die Folge: Bei einem ähnlichen – nicht durch einen Cyber-Angriff verursachten – unkontrollierten Herunterfahren eines Hochofens in Grossbritannien kamen drei Arbeiter zu Tode, weitere wurden verletzt.

ANSÄTZE ZUR SICHERUNG

Um professionellen Angreifern zu begegnen, sind strukturierte und umfassende Abwehrmassnahmen erforderlich. Zum einen muss die Systemarchitektur der Unternehmensnetzwerke besser an die erhöhten Sicherheitsanforderungen angepasst werden. Die Netzwerkverbindungen zwischen der Unternehmensführung und den einzelnen Produktionseinheiten sollten auf ein Minimum reduziert und Netzwerkzugriffsrechte limitiert werden. Vor allem der Datenverkehr mit dem ICS-Netzwerk sollte verstärkt überwacht werden, um Anomalien und Angriffe frühzeitig zu erkennen. Sehr hilfreich hierbei sind die Einrichtung von «Demilitarized Zones», also sicherheitstechnisch abgeschirmten Netzwerken, und der Ausbau des Network Security Monitorings. Auch sollten in den ICS sogenannte Canary Hosts eingerichtet werden, durch welche die IT-Sicherheit über jeglichen Zugriff von aussen informiert wird. So aufgestellt, verschwinden bereits viele Angriffsflächen, die Hackern leider meist zur Verfügung stehen. Werden dann noch für alle Netzwerke Krisenreaktionspläne aufgestellt, um bei einem Angriff schnell reagieren zu können, ist die Systemarchitektur bereits auf einem guten Weg. Doch muss auch das Personal ständig auf dem neusten Stand gehalten werden. Trainings und Fortbildungsmassnahmen sind unerlässlich. Schliesslich sollte auch der Informationsaustausch zwischen den IT-Sicherheitsexperten der Unternehmen gefördert werden. ←

ICS verstehen, Sicherheit schaffen

Wer sich in das Thema ICS und Sicherheit vertiefen will, kann dies im Rahmen eines Fortbildungskurses tun. Der nächste Kurs von SANS ist etwas für Schnellentschlossene – er findet bereits vom 4. bis 7. März in München statt. Dabei soll die bislang immer noch weitgehend bestehende Barriere zwischen dem Wissen um die Informationstechnologie und dem Wissen um die operative Ebene überwunden werden. IT-Sicherheitsexperte Justin Searle vermittelt zum einen erste Grundkenntnisse, Fachbegriffe und grundlegende Werkzeuge für den Umgang mit ISC, welche die Teilnehmer anschliessend auf die verschiedensten Industriebereiche und Industrieanwendungen übertragen können. Zum anderen werden Möglichkeiten vorgestellt, mit denen man den Sicherheitsstandard in den eigenen Netzwerken erhöhen und Netzwerkinfrastrukturen analysieren kann – etwa mit Command Line Tools für Windows und Linux.

Informationen zum Kurs ICS410: ICS/SCADA Security Essentials unter:
→ **www.sans.org/event/munich-2015/course/ics-scada-cyber-security-essentials**

«ICS sind zwar oft abgeschottet konzipiert worden, praktisch aber unkoordiniert vernetzt»

Michael Assante