Smart Meters kommen –

mit Sicherheit?

Smart Grids – zu Deutsch: intelligente Stromnetze – sind derzeit in aller Munde. Damit ist gemeint, alle Akteure auf dem Strommarkt durch das Zusammenspiel von Erzeugung, Speicherung, Netzmanagement und Verbrauch in einem Gesamtsystem zu vereinen. Um hierfür zukunftssichere Lösungen zu realisieren, müssen noch viele offene Punkte bedacht werden. Ein ganz wichtiger dabei ist die Sicherheit von Smart Metern, den kommenden digitalen Strom-Mess- und Steuerungsgeräten.

Von Prof. Dr. Hartmut Pohl und Ekkehart Gerlach

Smart Meter sollen kundenbezogene Informationen, wie die Verbräuche angeschlossener Geräte, sammeln und Informationen, wie z. B. Tarifierungsprofile der Energieunternehmen, speichern. Ziel ist, die Qualität zu steigern und mit flexiblen Tarifen und aktueller Angebotssteuerung Kosten zu sparen. Doch Kritiker glauben, dass intelligente Stromzähler zu viele Daten erheben können – beispielsweise, wann eine Wohnung von wie vielen Personen bewohnt und wann z. B. Fernsehen konsumiert wird. Sie befürchten, dass die Verbräuche manipuliert werden oder gar Hacker die Geräte abschalten können. Darüber hinaus sollen über die in jedem Haus installierten Smart Meter alle Stromanbieter mit allen Verbrauchern verbunden werden – also auch alle Endkunden untereinander.

Gründe gibt es also mehr als genug, Smart Meter besonders stark abzusichern. So müssen die Verbrauchsdaten der Kunden gegen unberechtigte Kenntnisnahme oder Auswertung und die Tarifdaten gegen Manipulation hinreichend geschützt werden. Die Steuerdaten im Smart Meter müssen so gesichert werden, dass z. B. der Strom nicht von Unberechtigten abgeschaltet werden kann. Und auch die Energieunternehmen müssen Angriffe aus dem Smart Grid verlässlich abwehren können.

Wie wichtig dieser Schutz ist, zeigen die leider erfolgreichen Angriffe auf Industriesteuerungen, die mit den im Internet übertragenen Würmern Stuxnet, Duqu, Flame, Mahdi, Gauss oder Shamoon sowie deren Nachfolgern, Varianten und Derivaten durchgeführt wurden. Es ist zu befürchten, dass zukünftig nicht nur – wie geschehen – weit entfernt liegende Uranzentrifugen angegriffen werden, sondern auch die Stromerzeugung und -verteilung in unserer Region.

Aber wie sieht es hierzulande mit der Sicherheit für Smart Metering aus? Konkrete Sicherheitsmaßnahmen hierzu werden von der „Technischen Richtlinie BSI TR-03109“ vorgeschrieben und auch mit dem „Protection Profile for the Gateway of a Smart Metering System“ bei der Evaluierung nach den sogenannten Common Criteria abgeprüft. Aber genauso, wie die Risiken in der klassischen Informationstechnik nicht alleine mit Firewalls, Intrusion Detection und Protection Systems, Antivirensoftware und Verschlüsselung abzuwenden sind, reichen auch hier die herkömmlichen Ansätze nicht aus. Stuxnet & Co. waren und sind deshalb erfolgreich, weil sie eine Reihe von bis dahin unbekannten Sicherheitslücken ausgenutzt haben. Daher müssen alle beteiligten Systeme – insbesondere aber das Smart Metering Gateway – mit geeigneten Verfahren zur Identifizierung bisher nicht erkannter Sicherheitslücken überprüft werden. Drei solcher Verfahren sind:

Architectural Analysis: Threat Modeling

Bereits im Design muss Sicherheit berücksichtigt werden. Nach einer vollständigen Analyse schützenswerter Komponenten sowie etwaiger Bedrohungen beginnt deshalb die Identifizierung und der Nachweis von Sicherheitslücken mit der Analyse der Dokumentation. Dazu gehört auch eine Untersuchung der Programmablaufpläne und der Datenflussdiagramme von und zu allen Kommunikationspartnern wie Stromherstellern und Verteilern bis hin zu Haushaltsgeräten, anderen Verbrauchern, Zählern und Anzeigeeinheiten.

Static Source Code Analysis

Dieses Verfahren wird Tool-gestützt durchgeführt. Analysiert wird der Source-Code (Whiteboxtest) der Zielsoftware, ohne ihn auszuführen – sogar bis hin zur semantischen Analyse. Damit ist es möglich, auch komplexe Fehler zu identifizieren, die etwa auf Race Conditions, Deadlocks oder falscher Pointer-Verwaltung basieren.

Dynamic Analysis: Fuzzing

Mit dieser „Blackboxtechnik“ werden Sicherheitslücken kostensparend ohne Kenntnis des Quellcodes frühzeitig identifiziert. Dazu werden geeignete Testdaten in das Zielprogramm eingespeist. Die Verarbeitung dieser Testdaten führt zu einem gewünschten fehlerhaften Verhalten des Zielprogramms (Crash, hoher Verbrauch an Ressourcen wie Rechenzeit). Dieses anomale Verhalten wird mithilfe eines Monitoringtoolsv protokolliert und voranalysiert. Sicherheitslücken werden durch Reproduzierung der Anomalie und Erstellen eines Exploits nachgewiesen. Für diese Technik wird ausschließlich der ausführbare Maschinencode benötigt.

Selbst wenn Smart Metering vielen noch als „Zukunftsthema“ erscheint, ist es höchste Zeit für den umfassenden Einbezug dieser Sicherheitsverfahren. Dies gilt umso mehr, da mit Smart Metering auch zusätzliche Mehrwertdienste möglich werden sollen. Die Sicherheit von Smart Metering darf nicht den Verbrauchern überlassen werden, die in der Regel mangels Fachwissen wohl nur für eine partielle oder lediglich vordergründige Sicherheit sorgen würden. Erst durch den Einsatz eines umfassenden Sicherheitskonzepts, das alle Aspekte der Sicherheit mit geeigneten Verfahren adressiert, können die Forderungen nach vertrauenswürdiger und sicherheitslückenfreier Software erfüllt werden. ■

__Prof. Dr. Hartmut Pohl__ ist Professor für Informationssicherheit/Softwaresicherheit an der Hochschule Bonn-Rhein-Sieg und geschäftsführender Gesellschafter der softScheck GmbH in Köln mit Sitz in Sankt Augustin. Das IT-Sicherheitsberatungsunternehmen ist seit mehr als zehn Jahren aktiv; einer der Beratungsschwerpunkte ist die Identifizierung bisher nicht erkannter Sicherheitslücken in Software und Hardware.

__Ekkehart Gerlach__ ist Geschäftsführer der deutschen medienakademie GmbH in Köln. Ziel der __Akademie__ ist es, als unabhängige und neutrale Fachakademie im Bereich von Kommunikation und Medien, insbesondere neuer Medien und neuer Technologien, Unternehmen wettbewerbs- und zukunftsfähiger zu machen.

Foto: Spectral-Design/Shutterstock.com