https://futurezone.at/science/spanische-smart-meter-koennen-einfach-gehackt-werden/91.479.373

Spanische Smart Meter können einfach gehackt werden

Spanische Sicherheitsforscher haben auf der Black Hat Europe einen Hack eines intelligenten Stromzählers gezeigt, mit dem ein Blackout verursacht werden kann.

In Spanien wurden bereits acht Millionen intelligente Stromzähler (Smart Meter) installiert, das sind rund 30 Prozent aller Haushalte. Zum Einsatz kommen dort Modelle der Firmen Endesa, Iberdrola und E.ON. Doch in Teilen Spaniens könnte es bald dunkel werden. Denn einer dieser Hersteller hat einen intelligenten Zähler im Einsatz, der leicht manipuliert werden kann, wie die beiden Sicherheitsforscher Javier Vazquez Vidal und Alberto Garcia Illera ***auf der Black Hat Konferenz in Amsterdam*** am Donnerstag aufgezeigt haben. Mit dem Hack der beiden Forscher lässt sich der Strom in einzelnen Haushalten abdrehen sowie die Stromrechnung manipulieren. Auch ein „Wurm“ lässt sich auf diesem Weg einspielen, mit dem man den Strom von vielen Haushalten gleichzeitig abdrehen und ein Blackout herbeiführen könnte.

Diese Attacke sei über einen fehlerhaften Code im umprogrammierbaren Speicherchip möglich, wie die Sicherheitsforscher sagen. Damit lasse sich die Hardware übernehmen, wie Vasquez Vidal erzählt. Beim Hack umgingen die beiden Forscher die Verschlüsselung des Zählers, eine relativ leicht knackbare symmetrische AES 128 Verschlüsselung.

Forscher selbst überrascht

Die Kommunikation zum Zähler würde dabei über Powerline laufen, so der Forscher. Genauere Details zum Hack wollten die Forscher jedoch nicht preisgeben, da diese die nationale Sicherheit gefährden würden. „Das Problem muss zuerst gelöst werden“, wie Garcia Illera betonte. Dies sei durch einen Remote-Zugriff auf die Zähler möglich, der Energieanbieter müsse zur Problembehebung nicht extra in die Haushalte seiner Kunden fahren. Die Forscher zeigten sich selbst überrascht darüber, was sie mit dem Zähler nach der „Übernahme“ in Folge alles anstellen konnten.

Das Szenario, das die spanischen Forscher gezeigt haben, könnte – theoretisch - auch in Österreich stattfinden, wie Markus Kammerstetter vom Institut für Rechnergestützte Automation an der TU Wien auf futurezone-Anfrage erklärt. Bereits vor mehreren Jahren warnte der Forscher vor dem Problem: "Das Problem ist, dass jegliche Kommunikation durch eine Software abgewickelt wird. Die Angreifer brauchen nur die Schwachstellen der Software zu finden und einen eigenen Code einschleusen", beschrieb Kammerstetter die technischen Möglichkeiten. "Alle Smart Meter eines Herstellers sind Software-technisch grundsätzlich gleich und daher ist es mit ein und derselben Schwachstelle möglich, auf vielen dieser Geräten einen

falschen Code einzuspielen." So sei auch die Entwicklung von Smart Meter-Botnetzen möglich, ***so Kammerstetter im Jahr 2011***.

Östereichische Geräte sind anders

Doch 1:1 lässt sich der Hack der spanischen Forscher nicht nach Österreich übertragen: „Fakt ist, dass sich das in Spanien eingesetzte Smart Meter System von den in Österreich eingesetzten Geräten technologisch unterscheidet. Die von den Kollegen entwickelten Angriffe können daher nicht direkt auf Geräten in Österreich angewendet werden“, sagt Kammerstetter.

In Österreich nehme man die Problematik sehr ernst, wie Kammerstetter betont. Dazu gibt es in Kooperation zwischen AIT und TU Wien mit ***(SG)² ein Forschungsprojekt***, das die Sicherheit von Smart Grid-Technologien sowie effektive Schutzmaßnahmen vor Cyber-Attacken in Österreich gründlich untersucht. Auch Kammerstetter gehört diesem Forschungsteam an. „Im Zuge der bisherigen Arbeit konnten wir bereits nachhaltige Verbesserungen gemeinsam mit Herstellern und Netzbetreibern erzielen“, erklärt Kammerstetter.

Untersuchungen an der TU Wien

An der TU Wien habe man zudem mit dem „Hardware Security Lab“ Pionierarbeit geleistet. „Dies ermöglicht es uns nicht nur Software-, sondern auch Hardware Angriffsformen (wie Powerline-Angriffe) auf eine Vielzahl von Systemen näher zu untersuchen, egal ob dies kritische Smart Grid Systeme und Smart Meter, drahtlose Bezahl- und Zutrittssysteme oder Wegfahrsperren von Kraftfahrzeugen betrifft. Einige unserer daraus erzielten Ergebnisse konnten wir bereits erfolgreich bei internationalen Top-Konferenzen publizieren“, so Kammerstetter.

Wie es um die Sicherheit der heimischen Smart Meter bestellt ist, wollte der Forscher jedoch nicht verraten. In Österreich kommen derzeit intelligente Zähler von Siemens, Echelon, Kaifa und Kamstrup zum Einsatz. „Nachdem das Thema Smart Metering und Smart Grid jedoch den Schutz kritischer Infrastrukturen und damit auch die nationale Sicherheit betrifft, unterliegen viele Ergebnisse unserer Arbeit strengen Geheimhaltungsvereinbarungen.“