



## "Stromnetze werden angreifbarer" - futurezone.ORF.at

---

Kategorie: SMART METERING | 02.12.2010 | Erstellt um 07:03 Uhr

---

**Die neuen, intelligenten Stromzähler stehen in Österreich kurz vor ihrer Einführung. Mit den falschen Funktionen an Bord würden sie allerdings das Stromnetz extrem anfällig für großflächige Angriffe machen, warnen Sicherheitsexperten. Ganze Straßenzüge könnten auf einmal ohne Strom sein, auch die Versorgungssicherheit steht am Spiel.**

Intelligente Stromzähler, sogenannte Smart Meter, werden in Österreich bald die mechanischen Ferraris-Zähler ablösen. Am Dienstag wurde dazu vom Parlament eine Gesetzesnovelle beschlossen, die es ermöglicht, dass die Zähler in Österreich eingesetzt werden. Sicherheitsexperten warnen jedoch davor, dass man als Land durch die neuen Geräte universell angreifbar werde. "Wir müssen uns darauf einstellen, dass wir im Stromnetz künftig mit ebenso häufigen Abstürzen rechnen müssen wie im Telefonnetz", meint der Datenschutzexperte Hans Zeger.

### Gesetzesnovelle in Österreich

In Österreich müssen bis 2020 80 Prozent der Haushalte mit intelligenten Stromzählern, sogenannten "Smart Metern", ausgestattet sein. Das schreibt eine Energieeffizienzrichtlinie der EU vor. Um diese in Österreich umzusetzen, musste das Elektrizitätswirtschafts- und -organisationsgesetzes (EIWOG) novelliert werden. Diese Novellierung wurde am Dienstag mit einer Zwei-Drittel-Mehrheit im Parlament beschlossen.

#### Mehr zum Thema:

- "Stromverbrauch interessiert viele gar nicht" ( <http://www.futurezone.at/stories/1664713/> )

Das neue System ist nämlich einerseits über eine Trafo-Station mit den Zählern von anderen Haushalten verbunden, andererseits aber auch mit den Datenmanagementsystemen der Energieversorger, die wiederum mit einem Online-Portal für Kunden verbunden ist. Dadurch gibt es für potentielle Angreifer viel mehr Zugriffspunkte- und ziele als zuvor. "Es gibt nicht eine Angriffsstelle so wie etwa beim Online-Banking, sondern viele Zwischenstellen", erklärt Zeger. Es lässt sich der Strom abdrehen, oder die Daten der Kunden werden über die Webportale abgegriffen, nennt Zeger potentielle Beispiele von drohenden Gefahren.

### USA: Trojaner über Smart Meter verbreitet

"Smart Metering-Systeme sind ganz normale IT-Systeme. Aus unserer langjährigen Erfahrung wissen wir, dass wir diese nicht zu 100 Prozent schützen können", erzählt Paul Karrer, Vorstand der Arrow ECS Internet Security AG und Sicherheitsexperte, der FUTUREZONE. Beispiele aus den USA hätten zudem gezeigt, dass Angriffe auf Stromnetze möglich sind. "In Kalifornien gab es einen Fall, bei dem ein Smart Meter andere Smart Meter mit einem Trojaner infiziert hat", ergänzt Joe Pichlmayr vom Sicherheitsunternehmen Ikarus. Ein weiteres Proof-of-

Concept-Beispiel hat gezeigt, dass über WLAN relativ einfach ein Schadcode eingeschleust werden kann, mit dem sich das komplette System übernehmen lässt.

## Land ohne Strom: In Österreich möglich?

"Man kann damit einem ganzen Land den Strom abschalten. Nichts würde mehr funktionieren, weil die gesamte Steuerung von den Angreifern kontrolliert wird", schildert Karrer ein mögliches Horrorszenario. Laut Reinhard Brehmer, Geschäftsführer der Wien Energie, sei dies in Österreich nur bedingt möglich, da es für die Größe des Landes viele verschiedene Netzbetreiber gäbe. Zudem sei es geplant, unterschiedliche Smart Meter einzusetzen, sodass nicht ein Gerät automatisch alle weiteren infizieren könne. Dennoch meint Brehmer: "Die Datensicherheit wird sicherlich unterschätzt."

Doch was kann man tun, damit unser Stromnetz nicht von Angreifern gekapert wird? "Gegen gezielte Angriffe helfen nur wirklich gute Konzepte und Strategien", meint Pichlmayr. Doch genau diese kosten. Nach jüngsten Schätzungen würde ein wirklich gut gesichertes Smart Metering-IT-System etwa zehn Prozent mehr kosten, als derzeit dafür geplant ist.

## Fernabschaltfunktion als Sicherheitsproblem

Vor allem eine Funktion ist maßgeblich dafür verantwortlich, dass Smart Metering-Systeme angreifbar werden: Die Fernabschaltfunktion. "Mit einer Remote-Abschaltung, die nicht abgesichert ist, lassen sich die Zähler relativ einfach manipulieren", meint Pichlmayr. Daher wäre es sinnvoll, wenn diese Funktion gar nicht erst im Smart Meter vorhanden ist." Durch eine derartige Funktion setze man die stabile Netzversorgung aufs Spiel, warnt auch Karrer. Er fordert daher: "Die Funktion muss hardwaretechnisch raus."

Die Zähler, die bisher bei den Testversuchen der Energieversorger verwendet wurden, haben eine derartige Fernabschaltfunktion von Haus aus eingebaut. Für die Stromlieferanten ist es schließlich bequem, wenn sie bei den Umzügen der Kunden nicht immer vor Ort erscheinen müssen, um den Stromverbrauch abzulesen. "Damit wird aber die Sicherheit des gesamten Systems aufs Spiel gesetzt, daher steht diese Ersparnis in keiner Relation", meint Pichlmayr.

## "Das ist keine X-Box, die geknackt wird"

"Es ist definitiv ein Unterschied, ob eine X-Box geknackt wird, oder ein DRM-Kopierschutzsystem, oder ob ein ganzes System, welches hinter einem Smart Meter liegt, gefährdet wird", versucht Pichlmayr den Ernst der Lage in Worte zu fassen. Ob die Systeme in Österreich über eine derartige Funktion verfügen werden, ist noch nicht geklärt. In der Gesetzesnovelle, die am Dienstag beschlossen wurde, werden derartige "Details" an das Wirtschaftsministerium und die Regulierungsbehörde E-Control abgewälzt. Bisher festgeschrieben wurde nur, dass das System "bidirektional" sein müsse. "Das alleine ist aber noch nicht böse", meint Pichlmayr.

## Verhaltensregeln für Datensicherheit

Der Datenschutzexperte Zeger spricht sich zudem für eine verpflichtende Einführung von Verhaltensregeln im Bereich der Datensicherheit aus. Eine ausschließlich verschlüsselte Datenübertragung, digitale Zertifikate, die Verwendung von anerkannten technischen Standards (wie etwa ISO 27001) und eine sicherheitstechnische Prüfung der Onlineportale soll etwa verpflichtend für alle künftigen Netzbetreiber sein. "Hier herrscht definitiv der größte Regelungs- und Handlungsbedarf", fügt Zeger hinzu.

"Je ausgeklügelter das System, desto besser", meint Pichlmayr. Sein Ziel ist es, durch die Schaffung des Bewusstseins für derartige Angriffe noch vor der Einführung der technischen Standards "diverse Designfehler zu vermeiden". Hoffentlich mit Erfolg - denn ansonsten könnte bald halb Österreich ohne Strom dastehen.

### Mehr zum Thema:

- "Stromverbrauch interessiert viele gar nicht" ( <http://www.futurezone.at/stories/1664713/> )

02.12.2010

"Stromnetze werden angreifbarer" - Fu...

(*Barbara Wimmer*)

Like

Be the first of your friends to like this.

3

AGB | IMPRESSUM DER FUTUREZONE GMBH