https://www.saurugg.net/2016/blog/stromversorgung/die-hackerdaemmerung-smart-meter-eine-gefahr-fuer-die-systemsicherheit

Die Hackerdämmerung – Smart Meter – eine Gefahr für die Systemsicherheit

12.Januar, 2016 |

Quelle: FAZ
Ein Stromausfall in der Ukraine könnte durch einen Cyber-Angriff ausgelöst worden sein. Es wäre das erste Mal, dass ein Stromnetz über das Internet lahmgelegt wurde.
Und erst im Dezember berichtete „Associated Press“ über Angriffe auf einen der größten Stromerzeuger in den Vereinigten Staaten. Dabei wurden Netzwerke geentert, über die das amerikanische Stromnetz gesteuert wird, und Passwörter sowie Dutzende Pläne von Kraftwerken und Stromnetzen erbeutet: Informationen, so die Nachrichtenagentur, mit denen man einen Stromausfall verursachen könnte.
„Um einen Blackout in größerem Maßstab durchzuführen, braucht man gutes Insiderwissen“, sagt der Darmstädter Sicherheitsexperte Kasper. Falle lediglich ein Kraftwerk aus, könne das Netz das ausgleichen. „Ein Angreifer kann aber über das Übertragungsnetz gehen, auf die Umspannwerke, auf die Leitstellen oder das Verteilnetz und versuchen, dort Kaskadeneffekte durchzuführen.“ Man kann das Stromnetz so treffen, dass sich der Schaden aufschaukelt und immer stärker wird.
Dass solche Kettenreaktionen möglich sind, zeigte ein Missgeschick im November 2006. Kaskadeneffekte können demnach in europäischen Netzen vorkommen. Aber wie realistisch ist es, dass Hacker sie hervorrufen und nutzen? „Potentiell“ sei die Gefahr hierzulande gegeben, sagt Kasper. „Das Bewusstsein dafür ist in der deutschen Industrie nicht ausreichend hoch, und wir sehen in unseren Bewertungen immer wieder Systeme, die mit zielgerichteten Angriffen aushebelbar wären.“ Allerdings bestehe keine Motivation für solche Attacken.
Trotzdem existieren Gegenmaßnahmen: Mitte 2015 beschloss der Bundestag das IT-Sicherheitsgesetz.
Strategien und Sicherheitsarchitekturen sind aber wenig hilfreich, wenn sie nicht umgesetzt werden, wie ein jüngeres Beispiel aus Europa zeigt. „Es gab Testinstallationen mit Smart Metern, die typischerweise Zehntausende Zähler umfassen“, erklärt Michael Kasper. Es handelte sich dabei um „intelligente“ Stromzähler, diese werden an ein Kommunikationsnetz angeschlossen und lassen sich fernsteuern. Weil sie als potentielle Einfallstore für Hacker gelten, sind sie umstritten. Auch in dem konkreten Fall ist etwas schiefgelaufen, erinnert sich der Sicherheitsexperte: „Es wäre möglich gewesen, sich mit einem speziellen Modem an das Netz zu hängen, dieses große Testsystem aus dem Tritt zu bringen und damit potentiell einen Lastabwurf zu erreichen.“ Die Abschaltung hätte passieren können, weil den Zählern eine Sicherheitsarchitektur fehlte: Die habe man schlicht vergessen.

Kommentar

Das Thema „Ukraine“ wurde bereits im Beitrag First known hacker-caused power outage signals troubling escalation analysiert. Das Problem bei diesen (Risiko-)Betrachtungen ist immer, dass diese so gut wie immer nur singulär erfolgen. Das heist, ein mögliches Auslöseereignis. Was aber wesentlich schwieriger – aber relevanter – ist, ist die kompination von mehreren möglichen Auslöseereignissen. Denn da sind wir dann in der Komplexität und bei systemischen Risiken, wo unsere Analysemethoden rasch an Grenzen stoßen. Siehe etwa Risk of financial crisis higher than previously estimated. Auch die Kettenreaktion/Dominoeffekt 2006 wurde nicht durch ein Einzelereignis ausgelöst, sondern durch eine Verkettung von mehreren an und für sich beherrschbaren Einzelereignissen. Und das vergessen wir leider allzu gerne. Dass ein reiner Cyber-Angriff gleich zum Dominoeffekt führen kann – ist möglich, wie die Leittechnikstörung 2013 gezeigt hat, auch wenn damals noch alles gut ging – aber in Kombination mit einer hohen Fragilität aufgrund einer etwa hohen Windstromeinspeisung (siehe Auswertung Redispatching & Intradaystops) könnte das wesentlich wahrscheinlicher sein. Daher geht es nur um die

Frage: **Wären wir darauf vorbereitet?** Auch die österreichische Gesellschaft und Industrie hat hier noch nachholbedarf … Blackout: Unternehmen sind schlecht vorbereitet.
Wie man die „Motivation für Angriffe“ beurteilt, dürfte wohl eher mit Kaffeesatzlesen zu tun haben, denn seriös lässt sich eine solche wohl kaum erheben. Und was auch heute stimmen mag, kann bereits morgen ganz anders aussehen. Das deutsche IT-Sicherheitsgesetz als Gegenmaßnahmen zu bezeichnen, ist wohl etwas hochgegriffen – siehe Im Blickpunkt: Das IT-Sicherheitsgesetz – Risikofaktor Scheinsicherheit.
Das Beispiel für die „Smart Meter“ Unsicherheit passiert natürlich nur im Labor und im Test. In der Wirklichkeit kann das nicht passieren … erst gestern dazu im Profil: Land am Strome.
Wir sorgen schon selbst für unsere Verwund- und Angreifbarkeiten und sollten daher nicht überrascht sein, wenn es wirklich mal passieren wird, wovon auszugehen ist. Die Lage ist aber nicht hoffnungslos – wir können etwas tun, auch bei einer Symbiose der IT-Vernetzung mit der Strominfrastruktur. Nur dazu müssen wir uns mehr um das Systemdesign kümmern (siehe etwa Umgang mit Komplexität oder Das Smart Grid im Zeitalter des Cyberwar).