Editorial/Kommentar

Sind über Fernabafrage oder Handys steuerbare Anwendungen wirklich sicher?

Freudig verkündeten Industrie und regionale EVU's in den letzten Wochen eine Zunahme der Nutzung von Smart-Metering. Besonders die EVU's sind daran interessiert, möglichst alle Privathaushalte mit Stromzählern auszustatten, die über Fernabfrage kontrolliert (abgelesen) werden können. Dem Wohnungsinhaber oder Mieter wird als besonderen Vorteil dieser Zähler die Kontrolllierbarkeit der Verbräuche sowie der damit verbundenen automatischen Rechnungsstellung genannt. Über die Risiken solcher Anlagen wird aber kaum ein Nutzer aufgeklärt. Denn die Fernabfrage läuft über Funk, vergleichbar mit der Nutzung eines Handys. Bekannt ist, dass Hacker nicht nur den heimischen PC, sondern auch so manches Handy ausspionieren (hacken). So hat Karspersky Lab festgestellt, dass täglich rund 315.000 neue Schadprogramme versuchen, Nutzer zu schädigen. Gerechnet wird mit einem stetigen größeren Zuwachs. Besonders bei Apps und Downloads stellen mobile Schädlinge eine große Gefahr dar. Dieser Gefahr aber sind auch alle durch Fernabfrage steuerbare Geräte im Wohnungsbau, wie Stromzähler, Brandmelder, Heizungsanlagen, Einbruchmeldeanlagen, usw., ausgesetzt.

Hans Jürgen Krolkiewicz, Foto privat

Vorinstallierte Viren auf fabrikneuen Rechnern und USB-Sticks werden bereits seit Jahren nachgewiesen. Allerdings ist dieser Nachweis extrem schwer und aufwändig darzustellen. Insbesondere muss jeder Nutzer (privat oder geschäftlich) von IT-Geräten permanent davor gewarnt werden. Fachleute sind der Meinung, dass viele Ausforschungen von Passwörtern durch ein vorinstalliertes Sniffing (ausspähen) erfolgt. Das macht die Fernabfrage von Geräten und Steuerungsanlagen im Wohnungsbau oder einem Online-Banking weniger vertrauenswürdig. Auch die nicht nur von privat oft genutzten Clouds sind oft Billigprodukte mit geringem Sicherheitsstandard. Deshalb sollten sensible und wichtige Daten dort niemals abgelegt werden. Nicht nur Unternehmen der Telekommunikation, sondern auch viele Hersteller von sicherheitsrelevanten Nutzungen, preisen die Vernetzung als „die Zukunft" an. Über die hochgelobte Cloud werde künftig eine totale Kommunikation ermöglicht, die ständige Kontrolle damit dem Nutzer gegeben. Dagegen weisen Fachleute darauf hin, dass heute eine solche Kommnukation nicht hinreichend sicherungsfähig ist. Besonders die Nutzung von iPhones und Androidgeräten zur Steuerung von Geräten und Anlagen in einem Gebäude ist noch immer mit einem großen Risiko verbunden. Trotzdem heben Hersteller von baulichen Sicherheitseinrichtungen in ihrer Werbung solche Möglichkeiten als besonderen Service an. Es ist egal, ob damit Rolläden hoch und runter gefaren werden können, die Raumheizung aus der Ferne kontrolliert werden kann (Energiesparen als Schlagwort), die Zuganskontrolle überprüft oder auf dem Handydisplay der Wohnungsinhaber sieht, wie seine Wohnung ausgeraubt wird – in allen Fällen ist es jedem IT-Fachmann möglich, über die nicht gesicherte Übertragung sich in die Anwendung einzuloggen (zu „hacken"). Und der Handynutzer wähnt sich in Sicherheit. Deshalb ist es wichtig, sich die Installation solcher Anlagen genau zu überlegen, solange es keinen einheitlichen Stadart für den Übertragungsweg gibt.

Hans Jürgen Krolkiewicz

Wie immer, bietet die führende Fachzeitschrift der Wohnungswirtschaft technisch fundierte Beiträge, wie sie bei Printmedien kaum zu finden sind. Und Sie können jederzeit in unserem Archiv auf alle früheren Hefte zurückgreifen, ohne umständlich suchen zu müssen. So etwas bietet ihnen bisher kein anderes Medium der Wohnungswirtschaft. Unser nächstes Heft 51 erscheint am 31. Dezember 2014

DIE REDAKTION WÜNSCHT ALLEN LESERINNEN UND LESERN EINEN GERUHSAMEN ADVENT!

PS: Sie sind anderer Meinung? Lassen Sie es mich bitte wissen!