Hakowanie żarówek jest możliwe

25 sierpnia 2013

Nowoczesne systemy sterowania oświetleniem są podatne na atak – twierdzi badacz Nitesh Dhanjani. Problem można rozwiązać już teraz, ale jest mała przeszkoda – nikt jeszcze nie wierzy, że takie luki mają znaczenie.

Jakiś czas temu „Dziennik Internautów” pisał o cyberataku na muszlę klozetową. Brzmi to jak zabawna ciekawostka i zapewne dlatego nikt się tym specjalnie nie przejął, nawet producent opisanej „inteligentnej” muszli.

Wczoraj ekspert od bezpieczeństwa Nitesh Dhanjani opublikował dokument dotyczący bezpieczeństwa nowoczesnych systemów oświetlenia. Mówiąc ściślej, badacz zajął się jednym systemem – Philips Hue. Jest on ogólnodostępny i łatwy w instalacji. Składa się ze specjalnych żarówek oraz kontrolera podłączanego do routera.

Mając ten system, można sterować oświetleniem za pomocą aplikacji mobilnej lub strony internetowej, na którą trzeba się zalogować. Żarówki Philips Hue mogą świecić na biało oraz różnymi kolorami, co daje wiele możliwości w zakresie dostosowania oświetlenia.

Nitesh Dhanjani ustalił, że Philips Hue ma luki w systemie uwierzytelniania, który umożliwia odbieranie komend ze smartfona. Wiedząc o tych lukach, Dhanjani stworzył złośliwy kod, który po zainstalowaniu na urządzeniu użytkownika może powodować ciągłe wyłączanie się światła. Wszystko wraca do normy, jeśli kontroler systemu Hue zostanie odłączony, ale wówczas tracimy korzyści, jakie daje „inteligentny” system oświetlenia.

Nitesh Dhanjani wcale nie twierdzi, że dokonał czegoś wielkiego i bardzo niebezpiecznego. Problem w tym, że jeśli inteligentne systemy oświetlenia będą bardziej powszechne, mogą pojawić się bardziej wyrafinowane formy ataków. Zgodzicie się zapewne, że nagłe wyłączenie oświetlenia w szpitalu byłoby kłopotliwe? Oczywiście w szpitalach nikt nie instaluje Philips Hue, ale chodzi o szerszy problem bezpieczeństwa systemów oświetlenia.

Ars Technica wspomina, że Nitesh Dhanjani usiłował zgłosić swoje odkrycia firmie Philips. Udało mu się wymienić kilka wiadomości na Twitterze w tej sprawie i na tym się skończyło. Można z tego wnioskować, że choć internet przedmiotów staje się rzeczywistością, producenci tych e-przedmiotów ciągle nie są przekonani, że jedną z ważniejszych cech ich produktów powinna być odporność na cyberatak.

Autor: Marcin Maj
Źródło: Dziennik Internautów