Internet rzeczy pozwala zaatakować sieć energetyczną

3 kwietnia 2021

Samochody elektryczne i inteligentne lodówki stwarzają zagrożenie cybernetyczne dla amerykańskich przedsiębiorstw produkcji energii elektrycznej, stwierdza raport Government Accountability Office. Zagrożenia nie są dobrze rozumiane przez badaczy, częściowo z powodu lokalnej i stanowej kontroli nad urządzeniami elektrycznymi pisze Patrick Tucker na portalu Defenseone.com

Pojazdy elektryczne i urządzenia domowe podłączone do Internetu sprawiają, że sieć elektryczna jest bardziej podatna na ataki cybernetyczne – a Departament Energii nie potrafi określić, jak bardzo poważny jest to problem, czytamy w marcowym raporcie Government Accountability Office (GAO).

Podczas gdy naukowcy zajmujący się cyberbezpieczeństwem od lat ostrzegają przed brakiem zabezpieczeń w urządzeniach podłączonych do tzw. „Internetu rzeczy", GAO twierdzi, że urządzenia te mogą zagrozić systemowi energetycznemu kraju: sieci elektrycznej dostarczającej energię elektryczną do domów i firm. Systemy te są zwykle zarządzane przez władze stanowe lub lokalne, podczas gdy urządzenia są kontrolowane przez konsumentów. Na tym polega część problemu.

„Przedsiębiorstwa energetyczne mają ograniczoną świadomość i wpływ na użytkowanie i cyberbezpieczeństwo tych urządzeń, ponieważ to konsumenci zazwyczaj je kontrolują" – czytamy w raporcie. Departament Energii „opracował plany wdrożenia krajowej strategii cyberbezpieczeństwa dla sieci, ale plany te nie uwzględniają w pełni zagrożeń dla systemów energetycznych".

Luki zabezpieczeniu w lokalnych sieci mogą zagrozić całemu systemowi lub sieciom regionalnym.

Sama liczba podłączonych urządzeń stanowi dużą część problemu, zwłaszcza jeśli napastnik może sprawić, aby działały w skoordynowany sposób. W 2018 roku naukowcy z Princeton University zademonstrowali możliwość przekształcenia wielu energochłonnych urządzeń – takich jak grzejniki i klimatyzatory – w botnet. Takie botnety są powszechnie wykorzystywane do internetowych ataków typu „odmowa usługi", które kasują dostęp do stron internetowych. Naukowcy z Princeton odkryli, że można ich również użyć „w celu manipulowania zapotrzebowaniem na moc w sieci".

Atak cybernetyczny na system energetyczny nigdy nie spowodował przerwy w dostawie prądu w Stanach Zjednoczonych, co Departament Energii zauważył w swojej odpowiedzi dla GAO. Jednak ataki wspierane przez Rosję doprowadziły do przerw w dostawie prądu na Ukrainie.

Na podstawie: DefenseOne.com
Źródło: Goniec.net