aut. Bartosz Józefiak 13.07.2016

POLITYKA KLIMATYCZNA OBAMY ZAGRAŻA CYBERBEZPIECZEŃSTWU SIECI PRZESYŁOWYCH USA

Możliwość potężnego cyberataku na amerykańskie sieci energetyczne rośnie. Powodem jest polityka administracji Baracka Obamy, która przeznacza potężne kwoty na rozwój zielonych źródeł energii, jednocześnie zapominając o zapezpieczeniach sieci przesyłowych przed cyberzagrożeniami.

Takie wnioski wypływają z raportu przygotowanego przez think tank Manhattan Institute. Urzędnicy pracują nad połączeniem energii z paneli słonecznych i farm wiatrowych w wart 6 trilionów dolarów system. Ten projekt stwarza jednak nowe podatności, które wrogie podmioty mogłyby wykorzystać do przeprowadzenia cyberataku.

Jak wyjaśniają dziennikarze portalu Flashcritic.com amerykańska sieć energetyczna nie tworzy póki co jednego systemu. Składa się ze skomplikowanej pajęczyny ośmiu regionalnych „supersieci", podłączonych do tysięcy regionalnych systemów przesyłowych. Do tej pory rząd wydał miliardy dolarów na stworzenie technologii integrującej sieci w jeden inteligentny system. Te działania mają na celu zwiększenie efektywności i ułatwienie centralnej obsługi przesyłu energii. Niestety, jak podkreślają autorzy raportu, projekt pozostawia wiele do życzenia w kwestii cyberbezpieczeństwa.

Oszczędności kosztem bezpieczeństwa

Operatorzy sieci również są przeciwko wydatkom na cyberbezpieczeństwo, ponieważ zwiększyłyby one koszty związane z obsługą krytycznej infrastruktury, a w konsekwencji mogły doprowadzić do wzrostu cen dla odbiorców. Eksperci dowodzą, że dzisiejsze oszczędności jutro mogą okazać się katastrofalne w skutkach.

Niebezpieczeństwo kryje się bowiem w przyszłym wykorzystaniu zielonych i „inteligentnych" sieci przesyłowych, które są połączone z internetem. Urządzenia służące do obsługi infrastruktury zostaną połączone ze sobą, tworząc sieć internetu rzeczy (Internet of Things, IoT). Wykorzystanie tej technologii oznacza jednocześnie otwarcie pola do działania dla cyberprzestępców. Zagrożenie jest realne, bo - jak czytamy w raporcie - łączna liczba cyberataków rośnie co roku o 60 proc. Dotyczy to także ataków na infrastrukturę krytyczną , której podejmują się zarówno cyberprzestępcy, hakerzy sympatyzujący z terrorystami jak i ci sponsorowani przez państwa wrogie rządowi USA. Badania firmy Cisco dowodzą, że blisko 70 procent menedżerów odpowiedzialnych za ochronę sieci przesyłowych przyznaje się, że doświadczyło co najmniej jednego naruszenia bezpieczeństwa.

Jak wyjaśniają dziennikarze portalu Flashcritic.com amerykańska sieć energetyczna nie tworzy póki co

jednego systemu. Składa się ze skomplikowanej pajęczyny ośmiu regionalnych „supersieci", podłączonych do tysięcy regionalnych systemów przesyłowych. Do tej pory rząd wydał miliardy dolarów na stworzenie technologii integrującej sieci w jeden inteligentny system. Te działania mają na celu zwiększenie efektywności i ułatwienie centralnej obsługi przesyłu energii. Niestety, jak podkreślają autorzy raportu, projekt pozostawia wiele do życzenia w kwestii cyberbezpieczeństwa.

Autorzy raportu sugerują, by powstrzymać się od rozwoju zielonych i inteligentnych sieci dopóki nie zostaną im zapewnione odpowiednie warunki do cyberobrony. Problemem jest jednak to, że sieci energetyczne kontrolowane są przez prywatne przedsiębiorstwa, które w całosci odpowiadają za bezpieczeństwo przesyłu. Szefowie firm muszą zdawać sobie sprawę z realności zagrożenia prowadzącego do całkowitego wyłączenia dostaw prądu do dowolnego regionu kraju. Autorzy raportu dowodzą jednak, że jak na razie raczej ignorują oni zagrożenie – wespół z rządową administracją. W styczniu Departament Bezpieczeństwa wWwnętrznego (Department of Homeland Security) opublikował raport dowodzący, że ryzyko groźnego cyberataku na sieci elektryczne jest niewielkie, a większym zagrożeniem są np. powalone drzewa.

Analitycy Manhattan Institute piętnują dysproporcje w rządowych wydatkach. Podają przykład: Administracja wydała 150 miliardów dolarów na rozwój zielonej energii, podczas gdy tylko 150 milionów dolarów pochłonęły badania nad cyberbezpieczeństwem. Według ekspertów cyberatak na krytyczną infrastrukturę w najczarniejszym scenariuszu może kosztować od 250 miliardów do 1 triliona dolarów. Takie byłyby koszty ogromnej awarii elektrowni i wyłączenia dostaw prądu.

Realne zagrożenia

Przedstawiciele wojska i służb zdają się być bardziej świadomi zagrożenia, niż administracja rządowa. Wojskowi z USCYBERCOM podkreślają, że poważny cyberatak na infrastrukturę krytyczną to tylko kwestia czasu. Takie próby były już zresztą podejmowane. W 2013 r. 34 - letni Irańczyk Hamid Firoozi włamał się do systemów nowojorskiej tamy Bowman. Przejął kontrolę nad systemami sterującymi śluzami i mechaniką konstrukcji. Haker włamał się do programu Windows XP, który był zainstalowany na komputerach obsługujących tamę. Nie było to zbyt trudne – z pomocą metody tzw. brute – force attack napastnik natrafił na banalnie proste hasło („666666"), potrzebne do zalogowania.

Firoozi dostał się do systemu decydującego o poziomie wody, temperaturze i podniesieniu lub opuszczeniu śluzy. Na szczęście tama w trakcie wszystkich prób ataku była odłączona od sieci i sterowana ręcznie w związku z pracami konserwatorskimi. Nie zmienia to faktu, że gdyby atak przeprowadzony był w innym momencie, napastnik z łatwością przejąłby kontrolę nad urządzeniami sterującymi poziomem i szybkością przepływu wody. To mogłoby spowodować poważne zagrożenia dla okolicznych mieszkańców. Firoozi jest wciąż poszukiwany przez FBI.

Najsłynniejszym jak do tej pory cyberatakiem na krytyczną infrastrukturę jest incydent, do którego doszło na Ukrainie w grudniu 2015 r. Wtedy to ukraiński przemysł energetyczny zainfekował trojan Black Energy, który spowodował m.in. wyłączenie dostaw prądu dla połowy populacji regionu Iwano-Frankowska (dawn. Stanisławów). Bez energii pozostały 103 miasta i miasteczka. Ten czarny scenariusz mógłby powtórzyć się też w innych elektrowniach na całym świecie – zwłaszcza, jeśli systemy przesyłowe będą podłączone do internetu rzeczy, który dziś jest największym wyzwaniem dla ekspertów od cyberbezpieczeństwa.

Czytaj też: Kto będzie odpowiadał za cyberobronę infrastruktury krytycznej USA?