Cyberdefence 24

aut. Tomasz Fastyn 22.07.2016

SEKTOR CHEMICZNY W USA OBAWIA SIĘ CYBERATAKÓW

Podczas 10 szczytu chemicznego w Stanach Zjednoczonych, który odbył się w dniach 19-21 lipca Andy Ozment z Departament Bezpieczeństwa Wewnętrznego USA (DHS) poruszył tematykę cyberbezpieczeństwa w infrastrukturze krytycznej.

– Każdy szef firmy, bez względu na branże w jakiej pracuje, powinien zapytać swój dział informatyki czy wszystkie systemy kontrolne są odpowiednio zabezpieczone. Przedsiębiorstwa muszą szczególnie pamiętać o zagrożeniu jakie znajduję się w cyberprzestrzeni, tak aby atak podobny do tego na Ukrainie nie zdarzył się w Stanach Zjednoczonych – powiedział 21 lipca podczas konferencji Andy Ozment.

Podobnie wypowiadają się eksperci cyberezpieczeństwa z Departamentu Bezpieczeństwa Wewnętrznego, którzy uważają że atak na ukraińską elektrownię powinien dać do myślenia przedstawicielom firm działających w obszarze infrastruktury krytycznej. Jednocześnie przyznali oni, że nie ma do tej pory sygnałów, aby takie ataki miały miejsce na terenie Stanów Zjednoczonych, jednak możliwość wykonania takiej operacji w kraju jest realna. DHS wysłał zespół składający się z informatyków śledczych, który zbadał jak hakerzy włamali się do systemu zarządzania elektrownią na Ukrainie. Atak, który miał miejsce pod koniec zeszłego roku i spowodował odcięcie od źródeł zasilania setki tysięcy obywateli Ukrainy na kilka dni.

Hakerzy jednocześnie podczas włamania postarali się, aby ponowne uruchomienie elektrowni nie należało do łatwych zadań. Podczas ataku usunęli z komputerów obsługujących przesył energii wszelkie możliwe dane, co spowodowało kompletny paraliż w dostawach energii na Ukrainie. Doprowadziło to do sytuacji, w której pracownicy elektrowni musieli manualnie aktywować stacje elektroenergetyczne oraz przesyłowe. Przed atakiem można było dokonać tego zdalnie.

– Cyberzabezpieczenia ukraińskiej elektrowni były na podobnym poziomie do instytucji zlokalizowanych na terenie Stanów Zjednoczonych. Wszystko było tam wykonane z zachowaniem odpowiednich norm bezpieczeństwa. Dlatego tak ważne jest zapewnienie jeszcze lepszego poziomu zabezpieczeń obecnych w sektorze chemicznym. Hakerzy posiadali odpowiednią wiedzę o całym systemie, nie poruszali się po omacku, dokładnie wyłączali te elementy infrastruktury, które mogły najbardziej zaszkodzić elektrowni – powiedział Andy Ozment z DHS.

Czytaj też: Polityka klimatyczna Obamy zagraża cyberbezpieczeństwu sieci przesyłowych USA