Cyberprzestępcy uderzyli w brytyjską infrastrukturę energetyczną

18 maja 2020

Jedna z kluczowych firm dla brytyjskiej energetyki, specjalizująca się w przesyłaniu energii Elexon, padła ofiarą cyberataku. W jego wyniku pracownicy stracili dostęp do e-maila i nie mogli zdalnie łączyć się z firmową siecią.

Przedsiębiorstwo ujawniło, że w wyniku ataku ucierpiała jedynie jego sieć wewnętrzna i laptopy zdalnych pracowników. Na szczęście nie ucierpiał ani BSC Centreal Systems, który zarządza dostawami energii, ani systemy podległej Elexonowi firmy EMR.

Na razie brak oznak, by atak mógł zakłócić brytyjski system energetyczny. Jest to jednak kolejny sygnał świadczący o rosnącej liczbie ataków na krytyczną infrastrukturę w Wielkiej Brytanii. W ciągu ostatnich tygodni National Cyber Security Centre wysłało do przemysłu kilka ostrzeżeń dotyczących cyberbezpieczeństwa. Agencja ostrzegła m.in. firmy farmaceutyczne i inne przedsiębiorstwa działające na rynku medycznym, że wspierane przez wrogie państwa grupy cyberprzestępcze wzięły na cel infrastrukturę związaną z walką z epidemią COVID-19. Podobnych problemów doświadczyły też Stany Zjednoczone.

Ataki na infrastrukturę energetyczną mogą mieć bardzo różne reperkusje. Od drobnych zakłóceń codziennej pracy po długotrwałe wyłączenia prądu obejmujące znaczne połacie kraju, co z kolei może niekorzystanie odbić się na działaniu innej krytycznej infrastruktury, np. szpitali. Dlatego też rządy wielu krajów powołały specjalne agendy mające za zadanie zapobieganie takim atakom i pomoc firmom w bronieniu się przed

nimi. Ponadto przedsiębiorstwa prywatne działające w krytycznych sektorach gospodarki są zobowiązane do posiadania odpowiedniej infrastruktury obronnej. W Wielkiej Brytanii firmy energetyczne mogą zostać ukarane grzywną w wysokości nawet 17 milionów funtów za brak odpowiedniej infrastruktury i reakcji.

Autorstwo: Mariusz Błoński
Na podstawie: ThreatPost.com
Źródło: KopalniaWiedzy.pl