Cyberdefence24

aut. Szymon Palczewski 03.06.2020

BAZA DANYCH BRYTYJSKIEJ FIRMY ENERGETYCZNEJ W SIECI

W ramach cyberataku na brytyjską firmę odpowiedzialną za kontrolowanie rynku oraz konsumpcję energii w kraju hakerom udało się wykraść wrażliwe informacje z wewnętrznych baz danych przedsiębiorstwa. Zgromadzone przez cyberprzestępców pliki zostały udostępnione w sieci. Incydent jest wynikiem braku odpowiednich cyberzabezpieczeń firmy.

Jak informowaliśmy wcześniej, władze Elexon, brytyjskiej firmy zajmującej się meteringiem, poinformowały, że przedsiębiorstwo padło ofiarą cyberataku, ale nie wpłynął on na zakłócenia w przepływie prądu, choć skutecznie zablokował zdolność przedsiębiorstwa do komunikacji z klientami. Równocześnie firma zadeklarowała, że od razu po wykryciu incydentu podjęto stosowne środki w celu rozwiązania problemu.

Obecnie wiadomo, że hakerom udało się wykraść wrażliwe informacje, które następnie zostały opublikowane w sieci. Wśród nich znajduje się między innymi plik pochodzący z wewnętrznej bazy danych firmy – donosi Computer Business Review (CBR), posiadający dostęp do skradzionych plików.

Opublikowane informacje obejmują również komunikację wewnętrzną personelu dotyczącą incydentu, co wskazuje, że hakerzy byli obecni w sieci jeszcze przez pewien czas po włamaniu.

Po cyberataku władze Elexon starały się załagodzić sytuację wskazując, że firma nie przechowuje żadnych danych na temat klientów. „Ponieważ nie przechowujemy żadnych danych na poziomie klienta, nie ma ryzyka dla użytkowników" – stwierdzono wówczas w oficjalnym komunikacie na stronie przedsiębiorstwa.

Brett Callow, CEO firmy Emsisoft, który ujawnił wyciek danych, powiedział w rozmowie z CBR, że często incydenty tego typu w firmach są wynikiem słabości samych zabezpieczeń. „Firmy często twierdzą, że padły ofiarą >wyrafinowanego cyberataku<, ale ataki te często udają się tylko z powodu podstawowych wad bezpieczeństwa, takich jak użycie słabych haseł, niestosowania MFA lub korzystania z źle zabezpieczonych serwerów internetowych" – wyjaśnia ekspert. – „Innymi słowy, znacznie ułatwiają życie cyberprzestępcom i narażają nie tylko dane, ale także informacje dotyczące ich klientów i partnerów biznesowych".

Czytaj też: Cyberatak na sektor energetyczny Wielkiej Brytanii