Cyberdefence 24

aut. Szymon Palczewski 20.03.2019

FIRMY ZBROJENIOWE I CZOŁOWY UNIWERSYTET OFIARĄ HAKERÓW

Jak informuje FBI, hakerzy oszukali w zeszłym roku dwa czołowe przedsiębiorstwa z sektora militarnego oraz jeden z głównych uniwersytetów wywołując straty w wysokości 150 tysięcy dolarów. Główną metodą działania cyberprzestępców było wysyłanie sfałszowanych e-maili.

Hakerzy podszywali się pod adresy e-mail wybranych organizacji, przekonując dostawców do dokonywania płatności przy użyciu fikcyjnych zamówień oraz dokumentów płatniczych. FBI jednak nie wymieniło z nazwy żadnej organizacji, która padała ofiarą cyberprzestępców.

W jednym z przypadków hakerzy, podszywający się pod pracownika czołowego uniwersytety, złożyli dwa zamówienia na 150 wyspecjalizowanych urządzeń cyfrowych, służących do mierzenia prądu. Dostawcą był Departament Obrony. Według FBI zdarzenie doprowadziło do strat w wysokości około 80 tysięcy dolarów. Pozostałe przypadki dotyczyły oszustw kontraktowych w sektorze obronnym o łącznej kwocie 90 tysięcy dolarów.

Według specjalistów strat można było uniknąć, gdyby „dostawcy zweryfikowali nazwy domen e-mail kupujących lub same adresy wysyłkowe, bądź gdyby zawiesili przesyłkę do momentu dodzwonienia się na podany numer telefonu kupującego”.

Oszustwa związane z fikcyjnymi e-mailami w sektorze biznesowym (BEC) stały się w ostatnich latach coraz bardziej złożone i wyrafinowane. „Oszustwa tego typu mają tendencję wzrostową, ponieważ są skuteczne” – wskazuje Alexander Heid, dyrektor ds. bezpieczeństwa w SecurityScorecard. „Istnieje zachęta dla hakerów – jest tam technologia (przyp. red. w przedsiębiorstwach), a ryzyko jest niskie w porównaniu z tradycyjnymi formami przestępczości. Teraz widzimy następstwa i ostrzeżenia organów ścigania po latach obserwowanej działalności” – tłumaczy ekspert.

W celu obrony przed oszustwami BEC, FBI sugeruje przedstawicielom firm weryfikację zamówienia m.in. za pomocą rozmowy telefonicznej. „Dostawcy powinni być szczególnie wyczuleni na nieznanych przedstawicieli firm, składających wnioski o wycenę za pośrednictwem strony internetowej dostawcy, bez późniejszego potwierdzenia przez nabywców zamówienia” – podkreślają specjaliści FBI.