**Hakerzy aktywni na wielu polach. Polskie firmy muszą uważać na dane w chmurze.**

**Cyberprzestępcy są coraz bardziej aktywni i kreatywni, obierając sobie za cel mobilne urządzenia wykorzystywane do celów firmowych – źródła danych i informacji o ogromnym potencjale. Na celowniku mają branże energetyczną, finansową, handlową – alarmują przedstawiciele Check Point. Przestępcy kierują się pobudkami finansowymi atakując firmy.**

Potwierdzają to dane CERT Polska - w 2018 roku doszło do ponad 3,7 tys. incydentów naruszenia cyberbezpieczeństwa. Oznacza to 17,5 proc. wzrost w ciągu roku. Wśród trzech, najczęściej występujących typów ataków należą: phishing, dystrybucja złośliwego oprogramowania i ataki na chmurę.

Według Check Point firmy w coraz większym stopniu przenoszą wykonywaną pracę oddziałów i aplikacje do chmury, dlatego muszą dostosowywać sieć SD-WAN tak, aby w sposób inteligentny przekierowywać ruch do usług w chmurze. Jednak bezpośrednie podłączanie oddziałów do chmury prowadzi do znacznego wzrostu zagrożeń oraz zwiększenia kosztów zarządzania IT.

Współczesne złośliwe oprogramowanie może przeniknąć do praktycznie każdej części infrastruktury informatycznej i rozprzestrzenić się w niej, w tym w lokalnych sieciach, w chmurze obliczeniowej, zdalnych biurach, urządzeniach mobilnych itd. Przykładem może być atak przy użyciu oprogramowania WannaCry, który dotyczył 300 000 komputerów w 150 krajach oraz NotPetya, który spowodował straty w wysokości 300 milionów dolarów dla zaatakowanych firm.

Hakerzy atakują dla celów finansowych. Przykładów jest wiele: Szpital w stanie Indiana w USA zapłacił 55 tys. dolarów okupu, żeby móc funkcjonować, Niemieckie biuro nieruchomości w Berlinie padło ofiarą kampanii ransomware, która zablokowała firmowe komputery pracowników i serwery a odblokowanie kosztowało firmę 300 tys. euro.

W lipcu br. w ciągu zaledwie dwóch tygodni przestępcy wyłudzili od władz dwóch miast na Florydzie (USA) ponad milion dolarów. W Lake City okup wyniósł około 500 tys. dol. i miał być wypłacony w bitcoinach. Władze podjęły ryzyko (nigdy nie wiadomo, czy hakerzy dotrzymają słowa) i przekazały pieniądze, aby uniknąć dalszego paraliżu w mieście. Atak był możliwy, ponieważ jeden z pracowników urzędu pobrał plik, który automatycznie zainstalował się na ‘’miejskim’’ komputerze.

Dlatego takie przedsiębiorstwa jak Apple zaproponowały oficjalnie hakerom współpracę. Pozwalają włamywać się do systemów firmowych i znajdować luki w zamian za wynagrodzenie. Najwięcej, bo aż 1 mln dolarów, dostanie ten, któremu uda się włamać do jądra systemu iPhone'a - iOS, ale pod warunkiem, że użytkownik smartfona nie musi wykonywać żadnych działań. 500 tys. dolarów dostanie ten, któremu uda się przeprowadzić atak sieciowy, ale także niewymagający akcji po stronie właściciela urządzenia. Hakerowi wypłacona zostanie dodatkowa 50-proc. premia, o ile znajdzie lukę w oprogramowaniu przed jego wydaniem.

Niezależnie od tego, z jakim rodzajem chmury mamy do czynienia, dominują ataki na aplikacje internetowe. Różnice między nimi polegają na poziomie zagrożenia. Praktyka pokazuje, że firmy potrzebują kompleksowych strategii zabezpieczających dane.

Przykład z ostatniej kampanii w Polsce nie pozostawia złudzeń. W wakacje mieliśmy do czynienia z falą maili z zawiadomieniem o rzekomej kontroli urzędu skarbowego. Maile ze złośliwym załącznikiem (trojanem Danabot) trafiały do skrzynek mailowych podatników. Wirus miał za zadnie wykraść m.in. loginy i hasła dostępowe do polskich rachunków bankowych. Nadawcą wiadomości był rzekomo Urząd Skarbowy, który informował o zamiarze wszczęcia kontroli. Skąd pochodziły bazy danych? Przypuszcza się, że wyciekły dzięki złemu zabezpieczeniu chmury, w której były przechowywane…