WIRTUALNE MASZYNY MOŻNA ZAMIENIĆ W BOTNET

Microsoft w ostatnim raporcie bezpieczeństwa (SIR) numer 21 potwierdził obawy wielu ekspertów na temat poziomu zabezpieczeń w maszynach wirtualnych oferowanych przez firmę. Problemem ma być brak odpowiedniego oprogramowania bezpieczeństwa przy implementacji chmury obliczeniowej w centrach danych.

Raport SIR 21 opisuje sytuację, jaka miała miejsce w pierwszym półroczu 2016. Wnioski z raportu nie są optymistyczne dla osób, które inwestują w rozwiązania chmurowe, szczególnie te wykorzystujące maszyny wirtualne. Po pierwsze liczba ataków na platformę chmurową znacznie wzrosła. W dodatku w przypadku udanego ataku na maszynę wirtualną jest ona wykorzystywana do rozsiewania złośliwego oprogramowania. W ten sposób tworzy się botnet działający w środowisku chmurowym.

Microsoft takie zjawisko nazwał *cloud weaponization*, co w dosłownym tłumaczeniu znaczy "uzbrojenie chmury obliczeniowej". Sieć maszyn wirtualnych skupiona w botnety może działać w identyczny sposób jak popularny Mirai, przeprowadzając ataki DDoS (ang. *distributed denial of service*), czy rozsiewając spam w sieci.

Większość incydentów mających na celu dostęp do chmury został zatrzymany przez platformę Azure, podkreśla Microsoft. Jednak inne firmy oferujące wirtualizację maszyn, nie są na tyle duże, aby mogły pozwolić sobie na opracowanie własnych mechanizmów bezpieczeństwa. Do tego dochodzą także koszty, związane z zakupem licencji na odpowiednie oprogramowanie. Nie daje to jednak gwarancji, że program nie zabierze maszynom wirtualnym niezbędnych zasobów, powodując gorsze działanie serwerów.

Czytaj też: ARMiR i Microsoft zbudują aplikacje mobilne

Rozwiązaniem, które ma zapewniać pełne bezpieczeństwo, jest wykorzystanie odpowiedniego oprogramowania klasy Light Agent wraz z pełną ochroną punktów końcowych, jak twierdzi Jewgienij Kasperski. Sama ochrona obecna w oprogramowaniu VMware vShield jest jego zdaniem niewystarczająca.