**Jak uchronić się przed kradzieżą wirtualnych kosztowności**

**Yoav Shay Daniely, product manager z centrum ochrony danych firmy Check Point wyjaśnia, dlaczego organizacje powinny zmienić podejście do zabezpieczania swoich definiowanych programowo centrów przechowywania danych**

W kwietniu 2015 roku miał miejsce jeden z największych rozbojów w dziejach: złodzieje obrabowali Hatton Garden - londyński depozyt, w którym klienci przechowywali swoją drogocenną biżuterię. Rabusie przebrani za robotników dostali się do budynku przez szyb windy i przebili przez betonową ścianę o grubości 50 centymetrów przy użyciu wiertarki elektrycznej, co umożliwiło im swobodny dostęp do strzeżonego skarbca wypełnionego biżuterią na ponad 48 godzin podczas wielkanocnego weekendu. Rozbrajając każda skrytkę depozytową dokonali zuchwałej kradzieży, której straty szacowane są na ponad 100 milionów funtów.

Co więcej, włamywacze początkowo uruchomili alarm, który został odnotowany przez policję. Mimo tego, nie znaleziono mechanicznych uszkodzeń na zewnętrznej części skarbca, które mogłyby wskazywać na włamanie, dzięki czemu przestępcy byli w stanie kontynuować napad. Innymi słowy, skok udał się dzięki wyłamaniu zewnętrznej ściany budynku – gdy tylko szajka dostała się do środka, nic nie stało na przeszkodzie by dyskretnie plądrować wnętrze skarbca.

Najcenniejszym majątkiem większości przedsiębiorstw nie są diamenty czy złoto, lecz dane. Nie składuje się ich w opancerzonych skarbcach – ich przechowalnią są centra danych. W wielu przypadkach zarówno centra danych jak i depozyty chronią się przed włamaniami w podobny sposób. Organizacje przykładają większą wagę do budowania coraz wyższych murów, zamiast zadbać o bezpieczeństwo od środka. Jeżeli atakujący jest w stanie naruszyć zewnętrzne zabezpieczenia, może wtargnąć do środka i manewrować między aplikacjami wykradając dane i zakłócając procesy biznesowe zanim zostanie złapany – tak samo jak rabusie plądrujący Hatton Garden, którzy swobodnie poruszali się po skarbcu pozostając niezauważonymi. W ostatnich napadach na centra danych hakerzy mieli dostęp do aplikacji i danych przez miesiące – właśnie dzięki niewykrywalności oraz braku środków bezpieczeństwa wewnętrznego.

**Wyzwania dla bezpieczeństwa w cyfrowym środowisku**

Sytuacja pogarsza się, kiedy przedsiębiorstwo odchodzi od fizycznych centrów danych i zamienia je na sieci wirtualne celem przyspieszenia konfiguracji i wdrażania aplikacji oraz redukcji kosztów związanych z zarządzaniem i utrzymaniem sprzętu. W nowym środowisku centrów danych, wszystkie elementy infrastruktury– sieć, przechowywanie danych, obliczenia oraz zabezpieczenia – uległy wirtualizacji i są dostarczane w postaci usług. Ta fundamentalna zmiana udowadnia, że tradycyjne podejście do kwestii bezpieczeństwa przestało się sprawdzać w przypadku dynamicznego, wirtualnego środowiska.

**Główne wyzwania dla bezpieczeństwa:**

· **Więcej połączeń wewnątrzbazowych–** Dawniej, większość ruchu generowały połączenia między klientem a bazą danych – takie połączenia były chronione tradycyjnymi środkami bezpieczeństwa. W dzisiejszych czasach, ruch wewnątrz centrów danych dramatycznie wzrósł razem z ilością aplikacji, które wymagają podtrzymywania nawiązanego połączenia i wymiany danych między sobą w celu poprawnego funkcjonowania. Wraz ze wzrostem ilości programów, hakerzy mają szerszy wybór celów do ataku: mogą skoncentrować się na jednej, niezbyt ważnej aplikacji i manewrować nią wewnątrz centrum bazy pozostając niewykrytym. W takim wypadku, zewnętrzne zabezpieczenia to za mało.

· **Ręczna konfiguracja i zmiany w polityce bezpieczeństwa:** w nowych, dynamicznych centrach danych, tradycyjne, manualne sposoby zarządzania bezpieczeństwem działają za wolno, a ich obsługa jest zbyt czasochłonna dla załogi IT. W rezultacie, kwestia ochrony przysparza dodatkowych problemów, które utrudniają napływ nowych aplikacji. Ręczna obsługa procesów naraża je na skutki błędu ludzkiego, przez co wzrasta ryzyko ataku. Dlatego ważne jest zautomatyzowanie zarządzania bezpieczeństwem, ponieważ pozwoli to w pełni wykorzystać potencjał bezobsługowych aplikacji i wzmocni sprawność centrum danych.

Do niedawna, wdrażanie zaawansowanych technologii, które chronią przed atakami i zapewniają bezpieczeństwo wewnątrz centrum danych, pociągało za sobą utrzymanie niezliczonej ilości oddzielnych sieci VLAN i nieustannego ręcznego konfigurowania i aktualizowania diagramów sieciowych. Krótko mówiąc, dla większości przedsiębiorstw były to zbyt trudne i kosztowne operacje.

**Mikrosegmentacja: uzbrojeni strażnicy wewnątrz skarbca**

A co jeżeli byłaby możliwość, aby umieścić odpowiednik ochroniarza w każdej skrytce bazy danych – wtedy nawet jeżeli wróg wtargąłby na nasz teren, wszystkie wartościowe zasoby wciąż byłyby objęte ochroną? Ponieważ centra danych są coraz częściej zarządzane programowo, ze wszystkimi funkcjami zarządzanymi w sposób wirtualny, możemy tego dokonać poprzez użycie mikrosegmentacji w SDDC (ang. software-defined data center – centrum danych zarządzane programowo).

Mikrosegmentacja polega na oznaczaniu kolorami i grupowaniu zasobów w centrum danych. Komunikacja pomiędzy tymi grupami objęta jest dynamicznymi metodami ochronnymi. Ruch w centrum danych jest potem kierowany do wirtualnych bram bezpieczeństwa, które – za pomocą zaawansowanych technik zapobiegania zagrożeniom – wnikliwie kontrolują zawartość ruchu sieciowego. Ma to na celu powstrzymanie prób przejścia atakujących z jednej aplikacji do drugiej wykorzystując dziury w oprogramowaniu. Dzięki temu, za każdym razem kiedy zostanie wykryta próba dokonania ataku przez maszynę wirtualną albo serwer, zostaną one oznaczone jako zainfekowane i natychmiast automatycznie przeniesione do kwarantanny przez „ochroniarza” centrum danych: bramę bezpieczeństwa. W ten sposób włamanie do systemu nie zagraża całej infrastrukturze.

Kiedy aplikacja zostanie dodana i ewoluuje, dla strategii bezpieczeństwa koniecznym jest, aby błyskawicznie zareagować i automatycznie dopasować się do dynamicznych zmian. Korzystając z integracji z chmurą oraz narzędziami do orkiestracji, program zarządzający ochroną w centrum danych uczy się roli aplikacji, jej wagi i lokalizacji. W rezultacie, za sprawą umożliwienia aplikacjom wewnątrz centrum danych bezpiecznej komunikacji między sobą, realizuje się odpowiednia strategia. Jeśli, przykładowo, dodawane są serwery lub zmienia się adres IP, obiekt jest już zabezpieczony i dziedziczy odpowiednie zasady bezpieczeństwa, eliminując potrzebę procesu ręcznego.

Wirtualizacja nie tylko napędza rozwój skalowanych, elastycznych, łatwych w zarządzaniu centrów danych, ale również sprzyja powstawaniu nowej generacji programów do ich ochrony. Dzięki używaniu mikrosegmentacji SDDC, dostarczanej przez zintegrowaną i zwirtualizowaną platformę bezpieczeństwa, zaawansowane usługi bezpieczeństwa i zapobiegania zagrożeniom mogą być dynamicznie stosowane wszędzie tam, gdzie są one potrzebne w środowisku centrów danych definiowanych programowo. To rozmieszcza uzbrojonych strażników wokół firmowego skarbca, strzegących każdego sejfu i ich cenną zawartość – aby centra danych nie padały ofiarą napadów w stylu Hatton Garden.