**Bezpieczeństwo chmury: wystarczy prosty błąd, by być narażonym na ataki**

**Dzięki nowemu hybrydowemu modelowi pracy obserwujemy, jak organizacje coraz częściej przenoszą swój “workload” do chmury. Transformacja ta zapewnia ogromne korzyści w zakresie elastyczności i skalowalności, ale wiąże się z nieodłącznym i zwiększonym ryzykiem bezpieczeństwa i zgodności. Prosty błąd konfiguracji może spowodować, że cała organizacja będzie narażona na zagrożenia ze strony hakerów, którzy - aby uzyskać dostęp do zasobów krytycznych - nie będą zmuszeni włamywać się do centrum danych.**

[Gartner przewiduje](https://www.gartner.com/smarterwithgartner/is-the-cloud-secure), że do 2025 r. 99% problemów związanych z bezpieczeństwem chmury będzie wynikiem błędu ludzkiego, popełnionego podczas konfigurowania zasobów i zabezpieczeń w chmurze. W czasach, gdy organizacje stają się coraz bardziej zależne od zewnętrznych dostawców chmury (również w kwestii bezpieczeństwa danych), takich jak AWS, Microsoft Azure, IBM i Google Cloud Platform, obawy związane z błędną konfiguracją i innymi lukami w chmurze mogą szybko się nasilać. Co więcej, w ciągu ostatnich dwóch lat wiele organizacji, uznających się za zagrożone, musiało przyspieszyć swoje procesy transformacji cyfrowej, co spowodowało luki w wiedzy oraz zasobach, które tylko pogłębiają obawy związane z bezpieczeństwem chmury.

W ramach modelu współodpowiedzialności — struktury bezpieczeństwa zaprojektowanej w celu zapewnienia odpowiedzialności za zagrożone dane i inne incydenty — dostawca chmury będzie oferować podstawowe zabezpieczenia, jednak to same firmy muszą zadbać o bezpieczeństwo własnych danych w chmurze. Innymi słowy, jeśli dostawcy usług w chmurze zapewniają, że „bramy miasta są zamknięte”, a teren jest dobrze strzeżony, to firmy nadal muszą zadbać o to, aby ich własne „drzwi do domostw” były zamknięte. To nie lada wyczyn, biorąc pod uwagę, że wiele dużych przedsiębiorstw polega obecnie na trzech lub czterech platformach chmurowych w ramach strategii wielu chmur.

**Nasilają się ataki na dostawców usług w chmurze**

Jak wskazano w [Raporcie Bezpieczeństwa 2022](https://pages.checkpoint.com/cyber-security-report-2022) firmy Check Point Software, w ubiegłym roku nastąpiła fala ataków, które wykorzystują luki w usługach wiodących w branży dostawców usług w chmurze. Dla zaangażowanych cyberprzestępców ostatecznym celem jest uzyskanie pełnej kontroli nad infrastrukturą chmury organizacji lub, co gorsza, całym zapleczem IT organizacji, w tym jej własnymi kodami czy danymi klientów. Nie trzeba dodawać, że może to mieć niszczący wpływ na dotknięte firmy i mają rację, że się martwią.

Rodzaje luk czy wad bezpieczeństwa, o których tutaj mówimy, nie są błędami logicznymi lub opartymi na uprawnieniach, wywodzącymi się z polityki kontroli organizacji, które mogą być wykorzystywane przez cyberprzestępców do uzyskania nieautoryzowanego dostępu i eskalacji uprawnień. Te mogły by być przynajmniej jednoznacznie wskazane i rozwiązane. Wady te są zwykle krytycznymi lukami w samej infrastrukturze chmury, przed którymi może być znacznie trudniej się zabezpieczyć.

Weźmy na przykład lukę OMIGOD, która otworzyła furtkę dla ataków na usługi w chmurze w 2021 r. We wrześniu wykryto cztery krytyczne luki w agencie oprogramowania Microsoft Azure, który umożliwiał użytkownikom zarządzanie konfiguracjami w środowiskach zdalnych i lokalnych. Szacuje się, że ten exploit zagrażał 65% baz klientów platformy Azure, narażając na niebezpieczeństwo tysiące organizacji i miliony urządzeń końcowych. Dzięki luce OMIGOD cyberprzestępcy byli w stanie zdalnie wykonać dowolny kod w sieci organizacji i eskalować uprawnienia administratora, skutecznie przejmując sieć. W ramach aktualizacji z września 2021 r. firma Microsoft rozwiązała problem, ale wydana przez nią automatyczna poprawka wydawała się nieskuteczna przez kilka kolejnych dni. W ciągu roku w usługach chmurowych Microsoft Azure ujawniono kolejne luki, w tym „ChaosDB”, która umożliwiła cyberprzestępcom odzyskanie kilku kluczy wewnętrznych, wykorzystywanych do uzyskania uprawnień administratora, które ostatecznie umożliwiłyby im zarządzanie bazami danych i kontami atakowanych organizacji. Wśród firm, które były narażone na te szczególne „otwarte drzwi”, znalazły się Coca-Cola, Skype, a nawet specjalizująca się w bezpieczeństwie firma Symantec.

Prawdopodobnie w 2022 r. pojawi się znacznie więcej podatności w zabezpieczeniach dostawców chmury, ale na szczęście istnieją możliwości będące pod kontrolą firm, które mogą zmniejszyć ryzyko.

**Zamykanie drzwi i wzmacnianie bezpieczeństwa wewnętrznego**

Zwiększenie zabezpieczeń chmury to nie tylko posiadanie odpowiednich produktów i usług, ale także pielęgnowanie „mentalności bezpieczeństwa” w całej organizacji. Niezależnie od tego, co mówi umowa dotycząca poziomu usług między organizacją a dostawcą chmury, to na organizacji ostatecznie spoczywa obowiązek zapewnienia ochrony dokumentacji klientów i innych ważnych danych.

Dlatego przed przeniesieniem do chmury obciążeń o znaczeniu krytycznym organizacje muszą upewnić się, że „drzwi” do ich aplikacji i danych są odpowiednio zatrzaśnięte. Oznacza to precyzyjne dostrojenie zarządzania tożsamością i dostępem, wdrożenie zasady „najmniejszych uprawnień”, tak aby dostęp do danych mieli tylko ludzie i aplikacje na zasadzie ścisłej potrzeby wiedzy. Oznacza to również lepszą segmentację sieci i wykorzystanie technologii firewall w celu zapewnienia, że wrażliwe dane mogą być odpowiednio „silosowane” i chronione w razie potrzeby.

Bezpieczeństwo w chmurze jest złożone, a w środowiskach z wieloma chmurami staje się jeszcze bardziej złożone. Warto więc pomyśleć o skonsolidowaniu wszystkich zabezpieczeń chmur różnych dostawców w jedno rozwiązanie, które monitoruje wszystkie złośliwe działania i zmniejsza obciążenie poprzez automatyzację typowych zadań, takich jak aktualizacje zasad. W idealnym świecie oznaczałoby to podejście „jednej szyby” do zarządzania bezpieczeństwem wszystkich zasobów w chmurze, dzięki czemu można uważniej przyglądać się incydentom związanym z bezpieczeństwem i skoncentrować wysiłki na tych, które budzą największe obawy.

Każde rozwiązanie bezpieczeństwa w chmurze jest tak dobre, jak stojący za nim silnik analizy, więc należy zapytać dostawcę, w jaki sposób radzi sobie z pojawiającymi się zagrożeniami i zagrożeniami typu zero-day. Przykładowo firma Check Point Software dysponuje rozwiązaniem ThreatCloud, które monitoruje miliony węzłów sieciowych na całym świecie i wykorzystuje ponad 30 technologii sztucznej inteligencji do identyfikowania zagrożeń w czasie rzeczywistym, dzięki czemu można je zablokować, zanim dostaną się do chmury, a nawet do sieci lokalnej lub użytkownika końcowego urządzenia.

Dodatkowo należy wprowadzić zabezpieczenia na najwcześniejszym etapie tworzenia aplikacji. Nie chcemy, aby kontrole bezpieczeństwa nadmiernie spowalniały DevOps i opóźniały wdrażanie aplikacji, ale równie dobrze nie możemy sobie pozwolić na cięcia w zakresie bezpieczeństwa. Podejście DevSecOps, które pozwala skanować kod pod kątem błędnych konfiguracji, a nawet złośliwego oprogramowania w ramach procesu DevOps, zapewni, że nie „upieczemy” podatności już na samym początku.

Przejście na chmurę może tylko przyspieszyć, gdy organizacje zdadzą sobie sprawę z korzyści, jakie przynosi ona w zakresie przewagi konkurencyjnej, elastyczności i odporności. Nadszedł też czas, aby przyjąć odpowiedzialne podejście do bezpieczeństwa i zgodności oraz wdrożyć je w chmurze. Jest to trudne i złożone zadanie, ale dobrą wiadomością jest to, że istnieją rozwiązania, które mogą nam w tym pomóc - nie tylko zabezpieczają sieć chmurową, ale także - dzięki wykorzystaniu sztucznej inteligencji i automatyzacji - zmniejszają nakład pracy związany z wykrywaniem i zapobieganiem zagrożeniom, nawet tym, które dopiero zostaną opracowane. Wreszcie, można to zrobić szybko, bo… wszystko jest w chmurze!