**Jak właściwie zarządzać systemem bezpieczeństwa w chmurze?**

**Nigdy wcześniej firmy nie były tak ściśle kontrolowane pod względem zbierania, przetwarzania i przechowywania danych i zasobów online. Organy regulacyjne, liderzy branży i użytkownicy oczekują, że dane osobowe będą skutecznie chronione przed niekontrolowanymi wyciekami i atakami. Koszt nieprzestrzegania przepisów, norm może okazać się bardzo wysoki, zarówno w kontekście przychodów, niezadowolenia użytkowników i jego wpływu na markę, kar czy kosztów odzyskiwania danych.**

Utrzymanie solidnego bezpieczeństwa stało się kluczowym wymogiem biznesowym w czasach, gdy krajobraz zagrożeń bezpieczeństwa jest trudniejszy niż kiedykolwiek. Dzisiejsze wysoce rozproszone aplikacje natywne dla chmury z efemerycznymi obciążeniami działającymi w złożonej infrastrukturze hybrydowej lub wielochmurowej stanowią rozległe i podatne ataki obszary dla cyberprzestępców.

W modelu współdzielonej odpowiedzialności dostawca usług zabezpiecza zasoby infrastruktury sieci, podczas gdy klient jest odpowiedzialny za bezpieczną konfigurację swoich kont i zasobów działających w infrastrukturze chmury publicznej. Rozwiązanie do zarządzania stanem bezpieczeństwa w chmurze klasy korporacyjnej (CSPM), które wykorzystuje narzędzia i usługi bezpieczeństwa natywne dla chmury, nie jest już jedynie nieoczywistym dodatkiem, a niezbędnym narzędziem do kompleksowego i dynamicznego wglądu w zgodność, korygowania błędów konfiguracji oraz proaktywnego zapobiegania zagrożeniom.

Dostawcy chmury oferują cenne usługi i narzędzia do zarządzania zgodnością (takie jak AWS Security Hub, AWS Config i Azure Security Center) oraz wykrywania zagrożeń (takie jak Amazon GuardDuty, AWS CloudTrail, Amazon Macie i Azure Sentinel). Wymienione usługi i narzędzia są jednak specyficzne dla dostawcy chmury. W infrastrukturze wielochmurowej/hybrydowej bardzo trudno jest je wykorzystać w celu uzyskania praktycznego, kompleksowego wglądu, niezbędnego do skutecznego zarządzania stanem bezpieczeństwa w chmurze. Dlatego tak ważne jest, aby platforma CSPM była w stanie głęboko zintegrować się z narzędziami natywnymi dla chmury i uwzględnić ich wyniki w scentralizowanym źródle wiedzy o stanie bezpieczeństwa.

Sprawdzona i skuteczna platforma CSPM może rozszerzyć zarządzanie stanem zabezpieczeń natywnych dla chmury również przez:

l **Częstsze i pełne skanowanie:** częstotliwość skanowania w czasie zbliżonym do rzeczywistego i automatyczne włączanie wszystkich wykrytych zasobów do obszaru skanowania.

l **Więcej ram zgodności i najlepszych praktyk:** Wbudowana obsługa pełnego zakresu ram zgodności i najlepszych praktyk, z możliwością łatwego dostosowywania wymagań do unikalnych potrzeb organizacji

l **Łatwe tworzenie reguł:** zamiast setek linii kodu, powinna to być intuicyjna metodologia tworzenia prostych i wyrazistych reguł

l **Wizualizacje z możliwością reagowania:** Inteligentna widoczność i wyraźna świadomość sytuacyjna, w tym automatyczna klasyfikacja zasobów wysokiego ryzyka, topologia w czasie rzeczywistym oraz wizualne śledzenie przepływu ruchu i działań użytkownika

l **Zaawansowaną ochronę proaktywną:** oparta na globalnej analizie zagrożeń, wykrywaniu anomalii w czasie rzeczywistym i alertach o włamaniach, szczegółowej kontroli uprawnień i podnoszeniu uprawnień oraz zautomatyzowanej naprawie

Autor: *Kristin Manogue, Check Point Software*