**Prowadzisz biznes w chmurze? Oto 4 podstawowe elementy kompleksowej ochrony**

**Cyfrowa transformacja zmusza biznes do szybszego niż kiedykolwiek wdrażania produktów. Jednak jaki jest tego koszt? Zespoły IT odczuwają ogromną presję, aby zrównoważyć szybkość z bezpieczeństwem. Chociaż wdrażają chmurę jako sposób na zachowanie elastyczności i skalowalności, to jednocześnie są bardziej podatne na cyberataki! Tylko w 2022 roku średni koszt naruszenia danych w samych Stanach Zjednoczonych wyniósł 9,44 miliona dolarów – zauważa Dotan Nahum z Check Point Software.**

W jaki sposób firma może zmniejszyć zależności, poprawić bezpieczeństwo i delegować zadania dostawcom, jednocześnie zwiększając szybkość rozwoju? Ekspert Check Pointa analizuje najnowsze trendy w branży i przykłady z życia wzięte, które pomagają stworzyć kompleksowy zestaw zabezpieczeń, niezależnie od tego, czy dopiero zaczynasz swoją przygodę z chmurą, czy chcesz jeszcze bardziej ulepszyć swój obecny zestaw zabezpieczeń.

**Zrozumienie krytycznych luk w zabezpieczeniach i zagrożeń dla firm działających w chmurze**

Od słabych haseł po niewystarczające zabezpieczenia, chmura zawiera szereg luk, które mogą wykorzystać cyberprzestępcy.

**1. Brak uwierzytelniania wieloskładnikowego (MFA)**

Usługa MFA zapewnia dodatkową warstwę zabezpieczeń w porównaniu z tradycyjnymi metodami uwierzytelniania jednoskładnikowego, takimi jak samo hasło. Jego brak jest istotną luką w zabezpieczeniach firm opierających swoją działalność o chmurę. Uwierzytelnianie oparte wyłącznie na hasłach można łatwo naruszyć poprzez ataki typu brute-force lub ponowne użycie haseł w wielu systemach, co skutkuje nieautoryzowanym dostępem do poufnych informacji lub zasobów przechowywanych w chmurze.

**2. Złośliwi „insiderzy”**

Zawsze istnieją osoby, które mają legalny dostęp do systemu, ale wykorzystują swoje uprawnienia do przeprowadzania złośliwych działań. Ataki wewnętrzne są trudne do opanowania, ponieważ odpowiedzialność nie spoczywa wyłącznie na barkach zespołów ds. cyberbezpieczeństwa. Działy HR i kierownicy powinni również wkroczyć, aby zarządzać niezadowolonymi pracownikami i ograniczać ryzyko sabotażu,

Aby temu zapobiec, należy wdrożyć ścisłą kontrolę dostępu i śledzić aktywność użytkowników pod kątem podejrzanych zachowań. Wskazane jest również posiadanie planu reagowania na incydenty z jasnymi procedurami wykrywania, badania i reagowania na incydenty.

**3. Rozproszone ataki typu „odmowa usługi” (DDoS).**

Ataki DDoS mają na celu wyłączenie usług internetowych poprzez zalewanie serwera przytłaczającymi żądaniami z różnych źródeł (zasadniczo go przeciążając). Powoduje to, że serwer nie jest w stanie odpowiedzieć na żądania, przez co usługa internetowa jest niedostępna.

Możemy chronić swoją firmę przed atakami DDoS, monitorując ruch w celu wykrycia nietypowych skoków, używając zapór ogniowych do blokowania złośliwego ruchu i mając systemy kopii zapasowych, aby usługi działały nawet podczas ataku.

**4. Niebezpieczne interfejsy API**

Interfejsy API odgrywają znaczącą rolę w tworzeniu bardziej połączonych i wydajnych doświadczeń cyfrowych. Ale jeśli API nie ma odpowiedniego uwierzytelnienia, może umożliwić nieautoryzowany dostęp do wrażliwych danych przechowywanych w chmurze, prowadząc do naruszenia danych i utraty poufnych informacji. Podobnie interfejsy API ze słabą lub uszkodzoną kontrolą dostępu mogą umożliwić atakującym ominięcie ustalonych ograniczeń.

Aby Twoje API było solidne, zaimplementuj MFA w całej organizacji i upewnij się, że wszystkie przesyłane dane są szyfrowane przy użyciu SSL/TLS. Musisz także uważać na to, kto ma dostęp do kluczy API.

**5. Błędnie skonfigurowane systemy i sieci**

Źle skonfigurowane systemy i sieci pozostawiają luki w środkach bezpieczeństwa i narażają wrażliwe dane. Zawsze dokładnie sprawdzaj [konfiguracje bezpieczeństwa przechowywania w chmurze](https://spectralops.io/blog/common-cloud-misconfigurations/), aby zapobiec takim lukom po skonfigurowaniu serwera. Co więcej, możesz zapewnić każdej osobie i narzędziu dostęp tylko do niezbędnego minimum informacji i zasobów, których potrzebują, aby skutecznie wykonywać swoją pracę.

**Dlaczego nie należy skakać od razu na głęboką wodę?**

Wybór idealnego stosu technologii ma kluczowe znaczenie dla każdej firmy działającej w chmurze, biorąc pod uwagę to, w jaki sposób może ona zrujnować lub zrujnować projekt. Ale przy tak wielu dostępnych opcjach wybór może być przytłaczający. Stąd potrzeba ustrukturyzowanego podejścia, aby każda podejmowana decyzja była dobrze przemyślana i uzasadniona. Oto kilka kroków, które należy wykonać, aby sfinalizować swój stos technologii:

**1. Określenie wymagań i celów projektu**

Przed sfinalizowaniem stosu technologii należy dokładnie zrozumieć, co projekt musi osiągnąć, całkowity koszt posiadania i oczekiwaną wydajność. Podczas tych dyskusji będziesz musiał na bieżąco informować interesariuszy, tak samo jak programistów, którzy będą ukończyć projekt.

**2. Ocena opcji technologicznych i ich przydatności dla projektu**

Po przygotowaniu wymagań projektowych należy teraz ocenić różne opcje technologiczne i ocenić ich przydatność. Obejmuje to rozważenie takich czynników, jak możliwości i ograniczenia technologii. Pomocne byłoby również przyjrzenie się poziomowi wsparcia dostępnego dla tej technologii (w tym wsparcie społeczności i dokumentacja) oraz jej ogólne przyjęcie na rynku.

**3. Skalowalność, koszt i bezpieczeństwo**

Stos technologii musi oferować możliwość rozwoju wraz z firmą, a nie go utrudniać. Można więc nadać priorytet technologiom z zaawansowanymi funkcjami bezpieczeństwa, takimi jak szyfrowanie danych (w spoczynku i podczas przesyłania), bezpieczne mechanizmy uwierzytelniania i autoryzacji oraz możliwość wykrywania naruszeń i reagowania na nie. Preferowane jest również, aby zbiór naszych technologii miał doświadczenie w zakresie regularnych aktualizacji w celu wyeliminowania ostatnich luk w zabezpieczeniach.

**4. Ocena kompatybilności z istniejącymi systemami i narzędziami**

Interoperacyjność między różnymi systemami i narzędziami jest niedocenianym czynnikiem, który może usprawnić procesy oraz pomóc zaoszczędzić czas i pieniądze, zapobiegając powielaniu wysiłków.

**5. Testowanie i ocenianie potencjalnych technologii poprzez weryfikację koncepcji**

Zawsze warto przetestować i ocenić potencjalne stosy technologii za pomocą weryfikacji koncepcji (POC). Oprócz zapewnienia programistom praktycznej wiedzy, pomoże to zidentyfikować wszelkie ograniczenia lub problemy, w tym wąskie gardła wydajności lub luki w zabezpieczeniach, a także zapewni cenny wgląd w to, jak pomyślnie wykorzystasz technologię w ostatecznym rozwiązaniu.

**Czy istnieje „idealny” zestaw technologii?**

Każda firma działająca w chmurze potrzebuje kompleksowego zestawu technologii zabezpieczających, aby utrzymać zaufanie swoich klientów i zminimalizować możliwość wystąpienia incydentu związanego z bezpieczeństwem. Powinien on obejmować kombinację technologii, procesów i narzędzi, które rozwiązują różne zagrożenia i luki w zabezpieczeniach. Oto kilka zalecanych elementów:

**1. Zarządzanie dostępem (IAM)**

IAM zajmuje się zarządzaniem cyfrowymi tożsamościami i ich dostępem do zasobów. W kontekście chmury odpowiada za zarządzanie tożsamościami użytkowników, aplikacji i usług wchodzących w interakcję z infrastrukturą chmury.

Narzędzia IAM zapewniają scentralizowane repozytorium informacji o tożsamości, umożliwiając administratorom definiowanie ról i uprawnień oraz egzekwowanie zasad [kontroli dostępu](https://spectralops.io/blog/examples-of-discretionary-access-control). Ponadto narzędzia te można zintegrować z innymi domenami bezpieczeństwa, takimi jak szyfrowanie i bezpieczeństwo sieci, aby pomóc firmom działającym w chmurze w przestrzeganiu różnych przepisów i standardów, takich jak RODO i PCI DSS.

**2. Pentesting**

Korzystając z narzędzi do testów penetracyjnych, Twój zespół IT może symulować atak, który naśladuje działania złośliwej strony trzeciej, oraz identyfikować luki i słabości w systemie docelowym. Wyniki mogą pomóc w ocenie odporności systemów na ataki w świecie rzeczywistym, zapewnieniu realizacji wymagań prawnych i ciągłej poprawie poziomu bezpieczeństwa. Poprzez regularne testy demonstrujesz również swoje zaangażowanie w bezpieczeństwo swoim użytkownikom i klientom.

**3. Broker zabezpieczeń dostępu do chmury (CASB)**

Podczas gdy tradycyjne rozwiązania bezpieczeństwa często nie mogą zapewnić odpowiedniej ochrony w dynamicznych i zdecentralizowanych środowiskach, CASB zapewniają ujednoliconą warstwę bezpieczeństwa, która znajduje się między dostawcą usług w chmurze a użytkownikiem końcowym. CASB pozwalają zachować kontrolę i widoczność zasobów w chmurze oraz zarządzać całym ruchem związanym z chmurą, zapewniając w ten sposób ochronę przed cyberzagrożeniami w czasie rzeczywistym.

**4. Baza danych w chmurze**

Bez wątpienia baza danych w chmurze jest koniecznością dla firmy działającej w chmurze. Działa ona na platformie przetwarzania w chmurze, a nie na sprzęcie lokalnym i jest zwykle zarządzana przez dostawcę usług w chmurze odpowiedzialnego za konserwację, aktualizacje i tworzenie kopii zapasowych. Bazy danych w chmurze ułatwią Ci pracę. Oto jak:

l **Scentralizowane zarządzanie:** Bazy danych w chmurze oferują scentralizowane i zautomatyzowane zarządzanie, co zmniejsza potrzebę ręcznej konfiguracji i konserwacji. Dzięki temu możesz zaoszczędzić czas i zasoby oraz skupić się na wynikach finansowych.

l **Duża dostępność:** Dostępność danych ma kluczowe znaczenie w każdym biznesie, zwłaszcza w środowisku chmurowym. Bazy danych w chmurze zapewniają automatyczne przełączanie awaryjne i replikację danych, dzięki czemu zasoby cyfrowe są chronione i dostępne przez cały czas.

l **Bezpieczeństwo:** możesz uzyskać dostęp do niezawodnych funkcji bezpieczeństwa, w tym szyfrowania, kontroli dostępu i audytu, korzystając z baz danych w chmurze, które pomagają chronić dane przed cyberzagrożeniami.

**Ustaw swoją firmę na sukces**

Zabezpieczenie firmy przed krytycznymi słabymi punktami i zagrożeniami ma kluczowe znaczenie dla zapewnienia jej długowieczności i sukcesu. Wybór odpowiedniego zestawu technologii jest kluczem do osiągnięcia bezpieczeństwa. Wybierając narzędzia, których potrzebuje Twoja firma, możesz poświęcić temu procesowi trochę czasu, biorąc pod uwagę kompatybilność, skalowalność i czynniki niezawodności. Przy prawidłowym stosowaniu Twój idealny zestaw technologii zmniejszy ryzyko naruszeń i zapewni bezpieczniejsze środowisko dla Twoich klientów i ich danych, a ponadto sprawi, że Twój sukces biznesowy będzie bardziej trwały.