Popularność wykorzystania chmury do przetwarzania danych rośnie, a system zarządzania sprzedażą online (Point of Sale – POS) jest obecnie coraz częściej wykorzystywany przez sprzedawców detalicznych. Oprócz tego, że przyspiesza on procesy biznesowe, jednocześnie może znacząco zminimalizować koszty!
Z reguły dostęp do systemu POS może być realizowany z użyciem każdego urządzenia, co pozwala sprzedawcy zaoszczędzić na zakupie drogiego sprzętu. Rozwiązanie w postaci oprogramowania opartego na chmurze, jest zazwyczaj dostarczane w formie usługi (Software as a Service), co wyklucza potrzebę instalacji i dalszego utrzymania środowiska uruchomieniowego – cały proces zostaje po stronie dostawcy.
Mimo że rozwiązanie chmurowe często jest już standardem w środowisku biznesowym, niektórzy sprzedawcy nadal nie są do niego przekonani i ciężko zwalczyć ich obawy nawet w obliczu korzyści płynących z przejścia na rozwiązania oparte o chmurę. Obalmy zatem 4 popularne mity najczęściej pojawiające się w dyskusjach o systemach w chmurze.

## Mit 1: Nie jesteś właścicielem swoich danych.

Nie jest to prawdą, pod warunkiem, że zostanie wybrany godny zaufania dostawca usług, który uszanuje prywatność przedsiębiorcy i nie użyje przechowywanych danych do celów marketingowych. Przeprowadzenie dobrej analizy podczas poszukiwań dostawcy, pozwoli uniknąć ryzyka z tym związanego. Należy zwrócić szczególna uwagę na możliwość wycofania swoich danych w przypadku rozwiązania umowy.

## Mit 2: Twoje dane są dostępne dla wszystkich.

Kluczem do rozwiania tej obawy jest jak w powyższym przypadku wybranie odpowiedniego dostawcy. Przy wyborze warto kierować się oferowanymi przez niego zabezpieczeniami i możliwością szyfrowania danych, co prawdopodobnie jest najlepszą gwarancją, że wszystkie zasoby są dobrze zabezpieczone. Do zaszyfrowanych informacji mają dostęp wyłącznie autoryzowane strony. W celu zapewnienia większego bezpieczeństwa zaufane chmury szyfrują dane zarówno podczas transmisji między użytkownikiem a usługą, jak i podczas ich składowania na nośnikach fizycznych serwerów. Przykładem jest np. platforma Microsoft Azure, która spełania normy ISO 9001:2015. Transmisja między użytkownikiem a platformą Azure jest realizowana z użyciem protokołu HTTPS, zaś składowane dane są szyfrowane z użyciem algorytmu AES z kluczami o długości 256 bitów, co zapewnia wystarczający poziom bezpieczeństwa.

## Mit 3: Duże ryzyko szkodliwego oprogramowania.

Obawy przed atakiem sprawiają, że ludzie nie są skłonni do przechowywania swoich danych w chmurze, podczas gdy powinno być zupełnie na odwrót. Trudno obronić się przed złośliwym oprogramowaniem, a jeszcze trudniej poradzić sobie ze skutkami ataku, jeśli nie posiada się wyspecjalizowanego zespołu IT, dostępnego 24/7.

Hakerzy mają łatwy dostęp do danych umieszczonych w ramach własnej serwerowni sprzedawcy (środowisko on-premises), jeśli nie jest wystarczająco dobrze chroniona. Drobni przedsiębiorcy często z powodu kosztów nie mogą utrzymywać wewnętrznego zespołu ekspertów odpowiedzialnych za bezpieczeństwo.

W środowisku chmurowym nawet niewielkie przedsiębiorstwa z ograniczonymi funduszami mogą wykorzystać inwestycje wielkich korporacji w cyberbezpieczeństwo. Znaczący dostawcy usług chmurowych korzystają z narzędzi do zapobiegania atakom typu DDoS (ang. distributed denial of service, blokada usługi) i pozwalają na wykrycie intruza, żeby chronić serwer przed zagrożeniami z sieci. Firmy te są na bieżąco zorientowane w kwestii pojawiających się nowych zagrożeń i stale dowodzą, że ich mechanizmy ochronne pozwalają na bezpieczne przechowywanie danych. Można w zupełności im zaufać, gdyż nie chronią jedynie danych, ale także swoją reputację.

## Mit 4: Nikt nie chroni danych przed kradzieżą i wypadkami.

Takie ryzyko często jest większe w przypadku lokalnych, niezarządzanych profesjonalnie serwerowni. Zabezpieczenie wymaga podjęcia odpowiednich kroków w celu zminimalizowania ryzyka kradzieży oraz wypadków skutkujących utratą danych. Wymaga to zainstalowania systemów monitorowania i alarmowania, co w praktyce dla wielu przedsiębiorstw jest trudne do wykonania, a także kosztowne.

Istnieje ryzyko, że komputer bądź serwer wraz z przechowywanymi danymi zostanie skradziony.

W takim przypadku następuje utrata wszystkich informacji, a także danych personalnych klientów, co może skutkować wstrzymaniem działalności do czasu odzyskania danych, powodując tym samym olbrzymie straty finansowe oraz wizerunkowe.

Ryzyko niesie ze sobą również fizyczne przechowywanie danych w ramach własnych serwerów. Problematyczne jest zapewnienie odpowiednich warunków w serwerowni, takich jak: odpowiednia temperatura, wilgotność czy też ciągłość dostaw prądu. Sprzęt jest także

podatny na innego rodzaju zniszczenia, chociażby wylanie kubka kawy na klawiaturę. Czy zatem można mieć pewność, że uda się zapobiec tym wszystkim ewentualnościom?
W przypadku zastosowania rozwiązania chmurowego dane są przechowywane poza fizyczną lokalizacją przedsiębiorstwa, gdzie są bezpiecznie i stale monitorowane pod kątem nieautoryzowanego dostępu fizycznego jak i wirtualnego. Trzeba mieć jednak świadomość, że nie zawsze jednak jest to najlepsze rozwiązanie – na ostateczny wybór powinnna mieć wpływ indywidualna ocena realnych potrzeb przedsiębiorstwa.
Podsumowując, chmura może wydawać się rozwiązaniem budzącym pewne obawy, jednakże odwaga często przyczynia się do zmian na lepsze. Wystarczy poświęcić trochę czasu na przeprowadzenie rozeznania, aby znaleźć godnego zaufania dostawcę. Zarówno profesjonalne Data Center jak i chmura publiczna dysponują certyfikatami bezpieczeństwa. Ważny jest również zakres możliwości wsparcia ze strony dostawcy. Dostępna pomoc jest istotna w codziennej pracy i optymalizacji procesów.
Artykuł przygotowany na podstawie materiałów ze strony LS Retail:
https://www.lsretail.com/blog/4-myths-dispelled-cloud-based-pos/