WYWIAD

Z GŁOWĄ W CHMURZE CZYLI JAK MĄDRZE ZADBAĆ O BEZPIECZEŃSTWO DANYCH OSOBOWYCH.

Na temat bezpiecznego przechowywania danych osobowych w chmurze obliczeniowej rozmawiamy ze Sławomirem Chmielewskim, Dyrektorem Biura Zarządzania Zgodnością, p. o. Dyrektora Bezpieczeństwa Korporacyjnego Orange Polska - wiodącego dostawcy usług telekomunikacyjnych w Polsce.

DM: Jako bodajże 3 firma w Polsce, Orange może się pochwalić certyfikacją systemu ISO 27018 - ochrona danych osobowych w chmurze obliczeniowej. Można powiedzieć, że na razie to certyfikat niszowy. Co miało wpływ na decyzję o wdrożeniu i certyfikacji systemu ISO 27018 w Państwa organizacji?

SCh: Nasi klienci przywiązują dużą wagę do ochrony informacji i mają sporo obaw związanych z „chmurą". Chcemy w ten sposób rozwiać ich wątpliwości. Mamy nadzieję, że dzięki temu przekonają się do tych usług i będą z nich częściej korzystać.

Chmura daje klientom wiele korzyści – przede wszystkim oszczędności oraz elastyczność i mobilny dostęp do najważniejszych informacji. Wzbudza jednak również obawy dotyczące ochrony informacji i prywatności, zwłaszcza w zakresie danych osobowych.

Dane osobowe obejmują szeroki zakres informacji. Oczywiste przykłady to np. nazwiska i dane kontaktowe lub nazwisko panieńskie matki, a z tych mniej oczywistych można wymienić m.in. adresy IP, wyciągi bankowe czy dokumentację medyczną.

Stosowanie międzynarodowych norm ISO/IEC 27018:2014 wraz z PN-ISO/IEC 27001:2014, daje naszym klientom pewność, że ich dane są należycie chronione i nie będą wykorzystywane do żadnych celów, na które nie wyrazili zgody.

DM: Czy podczas wdrożenia systemu napotkali państwo na jakieś problemy?

SCh: System Zarządzania Bezpieczeństwem Informacji ISO 27001 został wdrożony w Orange w 2006 roku, jeszcze w PTK Centertel, wówczas tylko dla usług mobilnych.

Stopniowo rozszerzaliśmy zakres tego systemu. W 2014 roku obejmował już część mobilną, jak i stacjonarną. W 2016 roku podjęto decyzję o rozszerzeniu certyfikacji o usługi przetwarzania danych osobowych w chmurze obliczeniowej (certyfikacja ISO 27018).

Przy tego rodzaju wdrożeniach trudno w 100% uniknąć trudności. Konieczne były na przykład korekty harmonogramu wdrożenia poszczególnych zabezpieczeń, ale ostatecznie osiągnęliśmy założony cel.

Było nim wdrożenie zarządzania bezpieczeństwem danych osobowych należących do naszych klientów zgodnie z najlepszymi międzynarodowymi standardami. Potwierdzeniem tego jest uzyskany certyfikat.

DM: Co to oznacza dla Klienta Orange? Czym teraz usługi chmurowe w ORANGE różnią się od konkurencyjnych?

SCh: Certyfikat, który uzyskaliśmy, potwierdza, że stosujemy skuteczne procedury bezpieczeństwa przy przetwarzaniu danych osobowych oraz, że efektywnie utrzymujemy certyfikowany system zarządzania bezpieczeństwem informacji.
Wdrożenie i utrzymywanie wymogów ISO/IEC 27018 daje naszym klientom m.in. pewność, że:

- Zachowają kontrolę nad swoimi danymi, będą mieć informację o ich położeniu geograficznym, a przestrzeganie przez nas wymagań normy to gwarancja, że dane osobowe są przetwarzane wyłącznie zgodnie z wymaganiami klienta, zapisanymi w umowie,
- Będą wiedzieć, co się dzieje z ich danymi. Przestrzeganie normy zapewnia przejrzystość zasad zwrotu, przesyłania i usuwania danych osobowych przechowywanych w chmurze,
- Zapewniamy skuteczną ochronę danych. Standard narzuca na nas ograniczenia dotyczące postępowania z danymi - przesyłania, przechowywania na nośnikach pamięci. Istnieją także odpowiednie procesy odzyskiwania i przywracania danych.
- Dane klienta zostaną wykorzystane tylko w takim celu, w jakim zostały nam powierzone.

To wszystko pozytywnie nas wyróżnia na tle innych firm.

DM: Czy pozytywny wynik audytu przybliża Was do spełnienia wymagań dotyczących rozporządzenia ogólnego w zakresie bezpieczeństwa danych osobowych, które zacznie obowiązywać pod koniec maja 2018.?

SCh: Tak, zdecydowanie.
Po pierwsze mamy efektywne zarządzanie systemem bezpieczeństwa informacji i co jest bardzo ważne, zarządzamy bezpieczeństwem systemowo z jednoznacznym podziałem ról i odpowiedzialności, opisanym w zasadach, procedurach, instrukcjach w obszarach spółki objętych zakresem SZBI. Prowadzimy regularne audyty bezpieczeństwa informacji, zarządzamy incydentami, szacujemy ryzyko w nowych projektach i przedsięwzięciach, szkolimy i podnosimy świadomość pracowników i współpracowników, cały czas doskonalimy nasz system.

Po drugie, otrzymaliśmy obiektywną ocenę tego, które obszary wymagają jeszcze pracy i doskonalenia wdrożonych procedur bezpieczeństwa.

Po trzecie, RODO wymaga przeprowadzania analiz ryzyka, a wdrożony i działający system (SZBI) przewiduje właśnie wykorzystanie narzędzia zapewniającego ciągłe doskonalenie w postaci analizy ryzyka dla projektów, inicjatyw i poszczególnych obszarów działalności firmy.

DM: Czy fakt, iż Orange ma certyfikowany system ISO 27001 ułatwiło uzyskanie pozytywnego wyniku ISO 27018? Pytam o to, czy warunkiem koniecznym do przystąpienia do certyfikacji ISO 27018 jest wcześniejszy wdrożony/certyfikowany system ISO 27001?

Tylko dzięki temu, że Orange posiadał swój systemem zarządzania bezpieczeństwem informacji (SZBI) oparty na normie bezpieczeństwa informacji PN-ISO/IEC 27001: 2014, efektywny, obejmujący całą naszą organizację i działający od 2014 roku, mogliśmy przystąpić do certyfikacji ISO 27018.

W typowej sytuacji podmiot wdrażający normę ISO/IEC 27001 chroni własne zasoby informacyjne. Jeśli jednak oferuje usługi przetwarzania danych w chmurze publicznej, jest odpowiedzialny także za dane powierzone mu przez jego klientów. Stąd konieczność dodatkowych zabezpieczeń.

W naszej ocenie, bez sprawnie działającego SZBI nie jest możliwe skuteczne wdrożenie normy ISO/IEC 27018. Celem tej normy, stosowanej w połączeniu z działaniami przewidzianymi w normie ISO/IEC 27002, jest stworzenie jednego, wspólnego zbioru środków kontroli bezpieczeństwa, które mogą wykorzystać dostawcy usług przetwarzających dane osobowe należące do klienta. Pozwala to na wdrożenie 114 zabezpieczeń SZBI, a następnie tylko uzupełnienie ich o wymagania wynikające z normy 27018.

DM: Jakich obszarów Państwa działalności dotyka certyfikacja systemu ISO 27018?

Oferta dla klientów biznesowych - czyli dla firm i instytucji obejmuje certyfikowane usługi, w których są przetwarzane dane osobowe w chmurach obliczeniowych:

- ICS (Integrated Computing Standard),
- ICM (Integrated Computing Managed),
- UCaaS (Unified Communication as a Service),
- smart CCaaS (smart Contact Center as a Service).

Integrated Computing to kompleksowe udostępnianie i zarządzanie infrastrukturą IT w modelu cloud computingu. Usługa oferuje wsparcie informatyczne dla klientów biznesowych. Występuje jako: Integrated Computing Standard (ICS) i Integrated Computing Managed (ICM). Pierwsza z tych usług jest przeznaczona dla firm zatrudniających pracowników IT i poszukujących dostępu do infrastruktury informatycznej. Drugi wariant to rozwiązanie oddające cały obszar IT w outsourcing wyspecjalizowanym integratorom.

UCaaS - polega na zintegrowaniu komunikacji głosowej, wideo oraz transmisji danych, jako zewnętrznej usługi (as a Service), świadczonej w modelu chmury obliczeniowej. Wykorzystuje urządzenia stacjonarne i mobilne do połączeń głosowych, może być również rozbudowana o kolejne elementy systemu takie jak komunikator pozwalający dzwonić i przesyłać pliki, zestawiane w prosty sposób tele i wideo-konferencje itd.

smart CCaaS - to usługa umożliwiająca obsługę klientów poprzez różne kanały komunikacyjne: kontakt telefoniczny, poczta elektroniczna, dialog internetowy (web chat), wspólne przeglądanie stron przez agenta i klienta (web collaboration), SMS i video. To także usługa świadczona w modelu chmury obliczeniowej.

DM: Jak wyglądał audyt? Czy opierał się tylko na sprawdzaniu dokumentacji czy obejmował obszar techniczny?

Usługa CCaaS oznacza „stanowiska agentów i supervisorów z chmury". Są one wyposażone w stacje robocze oraz telefony i tzw. softphone pracujące w standardzie SIP. Obsługa zgłoszeń przychodzących i wychodzących realizowana jest przez dostępne w chmurze serwisy, które zapewniają praktycznie wszystkie funkcjonalności Contact Center. Dodatkowo w oparciu o tę usługę można automatyzować procesy biznesowe korzystając przy tym z różnych mechanizmów komunikacyjnych. Jeśli chodzi o przetwarzane dane, ważne z punktu widzenia klienta, są to m.in. dane o ruchu, czasy rozmów, dane raportowe działania infolinii, konta agentów, nagrania rozmów.

Audyt sprawdzał zarówno istniejącą dokumentację, zasady, procedury, umowy, ale też ich praktyczne wykorzystanie i działanie.

Polegał na przeglądzie dokumentacji (pod względem jej aktualności i adekwatności), wizytacji stanowisk pracy oraz rozmowach z pracownikami i współpracownikami.

Audyt zgodności zabezpieczeń obejmował zarówno procesy realizowane przez HR, sprzedaż i inne jednostki organizacyjne, jak również obszar techniczny.

Audyt obszaru technicznego dotyczył z kolei weryfikacji fizycznych i technicznych (w tym IT) zabezpieczeń chmury obliczeniowej, stanowiącej miejsce przetwarzania danych osobowych, które powierzyli nam nasi klienci.

Weryfikowane były również zapisy umów podpisywanych z klientami, by mieli pewność co do transparentności naszego działania. Zapisy umowne muszą dokładnie precyzować miejsca, w których będą przetwarzane dane, a miejsca te podlegały audytowaniu.

DM: Na ile systemowe podejście do ogólnego problemu zapewnienia bezpieczeństwa informacji pomaga, a na ile jest barierą?

Systemowe zarządzanie umożliwia nam adekwatny do zagrożeń, wymagań biznesowych i prawnych poziom ochrony wszystkich informacji.

Dobór zabezpieczeń na podstawie analizy ryzyka zapewnia ich odpowiednią efektywność.

Jako operator telekomunikacyjny zdajemy sobie sprawę, że bezpieczeństwo informacji jest kluczowym elementem naszej wiarygodności, zaufania klientów, przewagi konkurencyjnej i oczywiście wymogiem prawa.

Dlatego też szczególną wagę przykładamy do zarządzania i nadzorowania bezpieczeństwa informacji, podziału ról i odpowiedzialności, systematycznego przeprowadzania analizy ryzyka utraty bezpieczeństwa informacji i monitorowania wdrożenia działań korygujących. Niezwykle ważne jest stałe dokonywanie analizy zagrożeń i oceny potencjalnych skutków, by na tej podstawie podejmować odpowiednie działania.

Należy również pamiętać o przeprowadzaniu planowych audytów bezpieczeństwa informacji, oraz szkoleniach i podnoszeniu świadomości pracowników w zakresie ochrony informacji.

Dziękuję za rozmowę! Rozmawiała Dagmara Machnicka

Przemysław Szczurek – Product Manager ds. Bezpieczeństwa Informacji TNP

Z ostatniego raportu zaprezentowanego przez Międzynarodową Organizację ISO wynika, że rynek certyfikacji bezpieczeństwa informacji dynamicznie się rozwija. Obserwujemy znaczące wzrosty zarówno w skali globalnej (ponad 20% wzrost r/r) jak i lokalnie w Polsce (wzrost 47% r/r). Wraz z rozwojem organizacji pojawia się coraz większa świadomość w zakresie bezpieczeństwa przetwarzanych informacji. Pojawiają się organizacje dla których ISO 27001 już nie wystarcza i dla usprawnienia wewnętrznych procesów związanych z bezpieczeństwem informacji sięgają do norm z rodziny 27000. Najbardziej popularne normy z rodziny 27000 związane są m in. z zarządzaniem ryzykiem, zarządzaniem incydentami bezpieczeństwa informacji, informatyką śledczą oraz te związane z bezpieczeństwem danych przetwarzanych w chmurze. Obecnie trwają prace nad nowymi normami: ISO/IEC SD 27103 — Information technology — Security techniques — Cybersecurity and ISO and IEC standards czy nad ISO/IEC 27102 — Information technology — Security techniques — Cyberinsurance. (albo po prostu: związanymi z Cybersecurity czy Cyberinsurance.)

Jak będą wyglądały kolejne lata? W mojej ocenie warto przyglądać się nowym standardom branżowym oraz wszelkim zmianom związanym z Industry 4.0