Outsourcing chmury dla podmiotów nadzorowanych – 9 kroków

Przedstawiamy esencję wiedzy dla podmiotów nadzorowanych na temat outsourcingu chmury. Są to praktyczne wskazówki dotyczące wymogów formalnych w procesie migracji do chmury, opracowane przez prawników z kancelarii Leśniewski Borkiewicz & Partners, w nawiązaniu do Komunikatu Urzędu Komisji Nadzoru Finansowego dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej.

KROK 1. PRZYGOTOWANIE KLASYFIKACJI I OCENY INFORMACJI

Dokument powinien identyfikować przetwarzane informacje, z podziałem na:

- informacje prawnie chronione w rozumieniu komunikatu UKNF (informacje związana z tajemnicami sektora finansowego wymienionymi w ustawach sektorowych);
- informacje, których ochrona wynika z innych uregulowań (np. RODO i dane osobowe, tajemnice przedsiębiorstw)
- informacje, które nie podlegają ochronie prawnej (np. publicznie dostępne opracowania / baza wiedzy)

KROK 2. OCENA CZY KOMUNIKAT UKNF ZNAJDUJE ZASTOSOWANIE

KROK 3. SZACOWANIE RYZYKA (ZGODNIE Z NORMĄ PN-ISO 27005)

Udokumentowanie kompleksowego szacowania ryzyka (identyfikacja, analiza oraz ocena zagrożeń, możliwości ich wystąpienia oraz wpływ tego wystąpienia na podmiot nadzorowany). Należy uwzględnić zarówno zagrożenia dla stosowania chmury jako takiej (np. awarie mechanizmów izolacji zasobów) jak również specyficzne zagrożenia, związane z zasobami

podmiotu nadzorowanego (np. brak zasobów ludzkich o ustalonych kompetencjach).

W tym kroku będą potrzebne informacje od dostawcy chmury, np. dotyczące możliwości korzystania z pomocy osób o specjalistycznych kompetencjach w obszarze cyberbezpieczeństwa jak i samej usługi chmury (szczególnie w sytuacji braku takich kompetencji wewnątrz własnej organizacji podmiotu nadzorowanego).

TIP: szacując ryzyko działaj w zgodnie z metodą: PDCA („plan – do – check – act")

KROK 4. ZARZĄDZENIE RYZYKIEM

Formalne zatwierdzenie wyników szacowania ryzyka. Zatwierdzenie powinno obejmować decyzję dotyczącą:

- usług chmury, z których podmiot nadzorowany będzie korzystał
- rodzaju i zakresu przetwarzanych w ramach tych usług informacji

KROK 5. PLAN PRZETWARZANIA INFORMACJI W CHMURZE

Opracowanie planu na podstawie wyników szacowania ryzyka, który będzie zawierał m.in.:

- opis przetwarzanych informacji
- sposób ich szyfrowania oraz zarządzania kluczami szyfrującymi
- zasady nadawania, kontrolowania oraz odbierania dostępu do informacji
- przewidywaną datę zawarcia umowy z dostawcą chmury, a jeśli jest już zawarta – referencje do tej umowy (numer, okres obowiązywania, data przedłużenia lub zmiany, data rozpoczęcia korzystania z usług)
- opis zadania realizowanego za pomocą chmury

KROK 6. POTWIERDZENIE, ŻE UMOWA Z DOSTAWCĄ SPEŁNIA WYMOGI KNF

W tym reguluje m.in.:

- deklarowane SLA
- metody zabezpieczenia lokalizacji przetwarzania (opis metod i narzędzi)
- prawo podmiotu nadzorowanego do przeprowadzenia inspekcji
- prawo dla nadzoru do wykonania obowiązków kontrolnych
- zasady wsparcia, w tym zakres i okna czasowe, tryb i sposób zgłaszania problemów z chmurą

KROK 7. POTWIERDZENIE, ŻE SAM DOSTAWCA SPEŁNIA WYMOGI KNF

Wymagania dla dostawców to przede wszystkim zgodności działania z normami (lub ich odpowiednikami):

- PN-ISO/IEC ISO 20000 dotyczące zarządzania usługami IT
- PN-EN ISO/IEC 27001 dotyczące zarządzania bezpieczeństwem informacji
- PN-EN ISO 22301 dotyczące zarządzania ciągłością działania
- ISO/IEC 27017 dotyczące bezpieczeństwa informacji w chmurze
- ISO/IEC 27018 dotyczące dobrych praktyk zabezpieczania danych osobowych w chmurze

Jeśli wynika to z szacowania ryzyka, można zaakceptować brak spełnienia części ww. wymagań.

KROK 8. URUCHOMIENIE USŁUG

Uruchomienie produkcyjne stosowania chmury powinien poprzedzać okres testowy, podczas którego na danych testowych (generowanych w przypadkowy sposób) testowane są scenariusze adekwatne do oszacowanego ryzyka.

KROK 9. POINFORMOWANIE UKNF

O fakcie korzystania z chmury należy poinformować UKNF, nie później niż 30 dni po rozpoczęciu świadczenia usługi.