Konferencja Naukowa

DZIAŁALNOŚĆ W ZAKRESIE CYBERBEZPIECZEŃSTWA. ASPEKTY PRAWNE, ORGANIZACYJNE I TECHNICZNE

Warszawa, 7 sierpnia 2020 r., godz. 10.00-14.00

Platforma komunikacyjna PTI - MS Teams PTI

ROZWÓJ RYNKU PODMIOTÓW ŚWIADCZĄCYCH USŁUGI Z ZAKRESU CYBERBEZPIECZEŃSTWA

Dr hab. Małgorzata Ganczar, Katedra Publicznego Prawa Gospodarczego, Katolicki Uniwersytet Lubelski Jana Pawła II

Obowiązki operatora usług kluczowych

Z art. 14 ustawy z 5.7.2018 r. o krajowym systemie cyberbezpieczeństwa wynika, że operator usługi kluczowej w celu realizacji niektórych zadań:

1. powołuje wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo (WSC) lub
2. zawiera umowę z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa.

Wymogi organizacyjne i techniczne

Powołania WSC lub zawarcia umowy z podmiotem wymaga realizacja zadań z zakresu:

1. wdrożenia przez operatora usługi kluczowej systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, zapewniający funkcje wymienione w art. 8 (np. prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem, wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, zbieranie informacji o zagrożeniach, zarządzanie incydentami itd.);

Wymogi organizacyjne i techniczne

Powołania WSC lub zawarcia umowy z podmiotem wymaga realizacja zadań z zakresu:

2. obowiązków operatora usługi kluczowej w zakresie wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, zapewnienia użytkownikowi usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową, w szczególności przez publikowanie informacji na ten temat na swojej stronie internetowej, a także przekazywania właściwemu organowi danych obejmujących informację określającą, w których państwach członkowskich Unii Europejskiej podmiot został uznany za operatora usługi kluczowej oraz datę zakończenia świadczenia usługi kluczowej nie później niż w terminie 3 miesięcy od zmiany tych danych;

Wymogi organizacyjne i techniczne

Powołania WSC lub zawarcia umowy z podmiotem wymaga realizacja zadań z zakresu:

3. obowiązków operatora usługi kluczowej określonych w art. 10 ust. 1–3, który w tym zakresie:
   - opracowuje, stosuje i aktualizuje dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej,
   - ma obowiązek ustanowić nadzór nad dokumentacją dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, a także
   - przechowuje dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej przez co najmniej 2 lata od dnia jej wycofania z użytkowania lub zakończenia świadczenia usługi kluczowej;

Wymogi organizacyjne i techniczne

Powołania WSC lub zawarcia umowy z podmiotem wymaga realizacja zadań z zakresu:

4. obowiązków operatora usługi kluczowej wymienionych w art. 11 ust. 1–3, czyli w zakresie m.in. obsługi incydentu, klasyfikacji incydentów, zgłaszania incydentu poważnego, współpracy z sektorowym zespołem cyberbezpieczeństwa itd.;
5. zgłoszenia incydentu poważnego zawierającego dane wymienione w art. 12;
6. informacji przekazywanych do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) w zakresie wymienionym w art. 13.

Wymogi organizacyjne i techniczne

Wewnętrzne struktury powołane przez operatora usługi kluczowej odpowiedzialne za cyberbezpieczeństwo oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa mają obowiązek:

1) spełniać warunki organizacyjne i techniczne pozwalające na zapewnienie cyberbezpieczeństwa obsługiwanemu operatorowi usługi kluczowej;
2) dysponować pomieszczeniami służącymi do świadczenia usług z zakresu reagowania na incydenty, zabezpieczonymi przed zagrożeniami fizycznymi i środowiskowymi;
3) stosować zabezpieczenia w celu zapewnienia poufności, integralności, dostępności i autentyczności przetwarzanych informacji, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów.

W przypadku zawarcia umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa, operator usługi kluczowej informuje właściwy organ i właściwy CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowy zespół cyberbezpieczeństwa o podmiocie, z którym zawarto umowę o świadczenie usług z zakresu cyberbezpieczeństwa, danych kontaktowych tego podmiotu, zakresie świadczonej usługi oraz o rozwiązaniu umowy w terminie 14 dni od dnia zawarcia lub rozwiązania umowy.

Wymogi organizacyjne i techniczne

Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo

Obowiązuje od 7 stycznia 2020 r. , dostosowanie pomieszczeń do 7 lipca 2020 r.

Uchylone rozporządzenie:
Rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo

Wymogi organizacyjne i techniczne

Przyczyny zmiany (za uzasadnieniem projektu rozporządzenia z 4 XII 2019 r.):

Poprzednio obowiązujące rozporządzenie „okazało się być trudne we wdrożeniu, nie dopuszczając niektórych form współpracy z ekspertami z zakresu cyberbezpieczeństwa.”
Wobec uzyskanych informacji z rynku, Ministerstwo Cyfryzacji zorganizowało spotkanie z przedsiębiorcami, podczas którego omówiono możliwości zmiany ww. rozporządzenia.
Uwagi zgłosiła m.in. Polska Izba Systemów Alarmowych, wskazując konieczność doprecyzowania niektórych przepisów, które wynikały z odniesień do norm technicznych. Zgłoszono potrzebę wprowadzenia następujących zmian:

- proporcjonalność wymogów (wymogi dostosowane do realizowanych obowiązków);
- usprawnienie istniejących wymogów;
- doprecyzowanie „miękkich zapisów” (np. rozbicie obowiązków typu „czynności z zakresu informatyki śledczej” na poszczególne obowiązki).

Wymogi organizacyjne

System bezpieczeństwa - chodzi o posiadanie, utrzymywanie i aktualizowanie systemu zarządzania bezpieczeństwem informacji spełniającego wymagania Polskiej Normy PN-EN ISO/IEC 27001 w zakresie obejmującym co najmniej świadczone usługi

Obsługa incydentu - chodzi o zapewnienie ciągłości działania usłudze obsługi incydentu oraz wsparcie operatorowi usługi kluczowej z czasem reakcji adekwatnym do charakteru usługi kluczowej

Deklaracja polityki działania - posiadać i udostępniać w języku polskim i angielskim deklarację swojej polityki działania w zakresie określonym dokumentem RFC 2350 publikowanym przez organizację Internet Engineering Task Force (IETF)

W zakresie realizowanych na mocy ustawy obowiązków dotyczących incydentów WSC lub podmiot zewnętrzny musi dysponować personelem posiadającym określone umiejętności – wątpliwości co do dokumentowania faktu dysponowania odpowiednim personelem – certyfikat, odbyte szkolenia???

Wymogi organizacyjne

Dysponować prawem do wyłącznego korzystania z pomieszczenia lub zespołu pomieszczeń w przypadku realizacji obowiązków w zakresie incydentów

Przeprowadzić analizę ryzyka mającą na celu dobór adekwatnych środków bezpieczeństwa fizycznego i technicznego pomieszczenia lub zespołu pomieszczeń, w których świadczone są usługi z zakresu cyberbezpieczeństwa, w której uwzględnia się wszystkie istotne czynniki mogące mieć wpływ na bezpieczeństwo w szczególności:

1) rodzaje informacji przetwarzanych w systemach teleinformatycznych;
2) otoczenie i konstrukcję budynków, w których będą świadczone usługi z zakresu cyberbezpieczeństwa;
3) liczbę osób mających lub mogących mieć dostęp do pomieszczenia lub zespołu pomieszczeń, a także posiadane przez nie uprawnienia oraz uzasadnioną potrzebę dostępu do pomieszczenia lub zespołu pomieszczeń;
4) szacowane zagrożenie sabotażem, zamachem terrorystycznym, kradzieżą lub inną działalnością przestępczą.

Wymogi techniczne

dwie grupy warunków technicznych:

1. **dysponować sprzętem komputerowym oraz wyspecjalizowanymi narzędziami informatycznymi** umożliwiającymi:

1) rejestrowanie zgłoszeń incydentów;
2) analizę kodu oprogramowania uznanego za szkodliwe;
3) badanie odporności systemów informacyjnych na przełamanie lub ominięcie zabezpieczeń;
4) zabezpieczanie informacji potrzebnych do analizy powłamaniowej pozwalające na określenie wpływu incydentu poważnego na świadczenie usługi kluczowej, …

2. **dysponować redundantnymi środkami łączności umożliwiającymi prawidłową i bezpieczną wymianę** informacji z podmiotami, dla których świadczą usługi oraz właściwym Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego działającym na poziomie krajowym.

Wątpliwości budzi ujęcie w § 2 ust. 2 rozporządzenia niektórych, sztywno określonych, wymagań w zakresie zabezpieczeń pomieszczeń lub zespołu pomieszczeń pomimo oparcia ich doboru na podstawie przeprowadzonego szacowania ryzyka.

Dziękuję za uwagę!
mganczar@kul.pl