UCHWAŁA nr 1

RADY do SPRAW CYFRYZACJI

z dnia 19 lipca 2019 r.

dotycząca projektu rozporządzenia Ministra Cyfryzacji zmieniającego rozporządzenie w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo.

Na podstawie art. 17 ust. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz .U. z 2019 poz. 700, ze zm.) oraz § 5 Regulaminu Rady do Spraw Cyfryzacji stanowiącego załącznik do Zarządzenia nr 1 Ministra Administracji i Cyfryzacji z dnia 5 stycznia 2015 r. w sprawie ustanowienia regulaminu prac Rady do Spraw Cyfryzacji (Dz. Urz. z 2015 r. poz. 1, ze zm.), uchwala się, co następuje:

W związku z pracami nad zmianą rozporządzenia w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, Rada ds. Cyfryzacji pozytywnie ocenia inicjatywę nowelizacji zapisów służących określeniu wymagań mających wspierać bezpieczeństwo kluczowych z punktu widzenia funkcjonowania Państwa usług.

Jednocześnie zwracamy uwagę na kilka elementów przedmiotowego projektu, które wymagają w naszej ocenie ponownego rozpatrzenia, w szczególności:

1. W § 2 przedmiotowego projektu określono zakres czynności wykonywanych przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa, które mają być wykonywane wyłącznie w pomieszczeniach posiadających odpowiednie zabezpieczenia. Uzasadnienie do projektu rozporządzenia doprecyzowując zakres przedmiotowych działań wyraźnie wykracza poza odpowiednie zapisy art. 14 ust. 2 pkt 2 ustawy o krajowym systemie cyberbezpieczeństwa. Przywołany zapis ustawy wyraźnie precyzuje, iż tylko działania związane z reagowaniem na incydenty powinny być dokonywane w odpowiednio zabezpieczonych pomieszczeniach. Natomiast zapis projektu Rozporządzenia poszerza zakres przedmiotowych czynności.

   W związku z powyższym zwracamy uwagę, że należy rozważyć możliwość odpowiedniej zmiany treści § 2 przedmiotowego Rozporządzenia i nadać mu brzmienie zbieżne z treścią art. 14 ust. 2 pkt 2 ustawy o krajowym systemie cyberbezpieczeństwa.

2. W odniesieniu do wymagań dla podmiotów posiadających status operatora usługi kluczowej, a więc zobowiązanych do powołania wewnętrznych struktur cyberbezpieczeństwa i mogących świadczyć usługi cyberbezpieczeństwa dla innych operatorów usług kluczowych, § 1 określa, że taki podmiot musi „posiadać i utrzymywać w aktualności system zarządzania bezpieczeństwem informacji spełniających wymagania Polskiej Normy PN-EN ISO/IEC 27001", a także „zapewnić ciągłość działania usłudze obsługi incydentu, polegającej na podejmowaniu działań w zakresie rejestrowania i obsługi zdarzeń naruszających bezpieczeństwo systemów informacyjnych zgodnie z wymaganiami Polskiej Normy PN-EN ISO22301". Dostrzegamy w tym zapisie pewną sprzeczność, a mianowicie, Norma ISO/IEC 27001 jako zasadę wdrażania wszystkich zabezpieczeń wskazuje konieczność uzasadnienia ich wdrożenia w oparciu o przeprowadzoną analizę ryzyka i szans. Natomiast nawet jeśli przeprowadzona w ten sposób analiza ryzyka nie potwierdzi wykonania zabezpieczeń zgodnie z § 2, to i tak będą one wymagane. Sprzecznością wydaje się fakt przywołania ISO/IEC 2701 i jednoczesne narzucenie sztywnych zabezpieczeń fizycznych.

   Proponujemy, w celu uniknięcia ewentualnych wątpliwości, rozważenie możliwości określenia wykazu zabezpieczeń jako listy przykładowej, od której dopuszczalne są wyjątki uzasadnione szacowaniem ryzyka.

3. W §3 pkt 1 lit. c „badanie odporności systemów informacyjnych na przełamanie zabezpieczeń" – wydaje nam się, że powinno się wskazać również „ominięcie zabezpieczeń". Generalnie – „przełamanie" i „ominięcie" to pojęcia, którymi posłużono się w art. 267 § 1 kk. Mają się one dopełniać (trudno odróżnić „przełamanie" od „ominięcia") – dlatego jak sięga się do terminologii kk należy użyć obu. Zauważyć jednak należy, że – jak słusznie podkreślają informatycy – czegoś takiego jak złamanie zabezpieczeń, czy ominięcie w informatyce nie ma. Należy rozważyć czy nie właściwsze byłoby sięgnięcie do terminologii uKSC i użycie terminu „podatność", czyli np. „wykorzystanie podatności". Jeżeli można przyjąć, że np. złamanie hasła jest wykorzystaniem podatności. Ale na pewno w tym pojęciu mieści się „ominięcie zabezpieczeń" (czyli np. wykorzystanie luk, m.in. poprzez wprowadzenie nieprzewidzianych danych prowadzących np. do przepełnienia buforów pamięci).

4. W § 3 pkt 1 lit d „zabezpieczania informacji potrzebnych do analizy powłamaniowej pozwalające na określenie charakteru, zakresu i czasu trwania incydentu na potrzeby postępowań prowadzonych przez organy ścigania". Pojęcie „informacji" – uważamy, że bardziej trafnym będzie zastosowanie pojęcia „danych informatycznych" (chodzi tu przede wszystkim o logi) lub ewentualnie „danych informatycznych i informacji" – wtedy w pojęciu „informacji" mieszczą się jakieś „informacje" niemające postaci danych informatycznych, o ile jest taka konieczność. Pojęcie „informacji" miałoby charakter dopełniający.

   Dodatkowo w przedmiotowym zapisie należy doprecyzować pojęcie „zakres", gdyż można mówić o „zakresie terytorialnym" czy „zakresie czasowym". Jednak ten „za-

kres” został wyłączony z zakresu tego pojęcia – bo dalej mowa o „czasie trwania”. Dlatego konsekwentnie trzeba chyba uściślić stosowanie i rozumienie tego pojęcia w przywołanym przepisie. Zwłaszcza, że przez „zakres” rozumie się chyba w tym wypadku np. liczbę dotkniętych użytkowników, a to nie jest normalne, potoczne rozumienie. Dlatego może warto odwołać się, nawet przykładowo, do liczby użytkowników, zaatakowanych hostów. Wówczas jednak warto rozważyć zmianę pojęcia na „zasięg”.

5. Podobnie jak w pkt 2 rekomendujemy rozważenie modyfikacji § 5, który odnosi się do możliwości wykonywania obowiązków poza zabezpieczonymi pomieszczeniami w formule pracy zdalnej. Ponownie przywołujemy w tym kontekście zapisy Normy ISO/IEC 27001, która określa, że odpowiednie zalecenia dla bezpieczeństwa pracy zdalnej wdrażane są w uzależnieniu od szacowania stopnia ryzyka.
6. Proponowane w § 6 i § 8 określające terminy na dostosowanie się podmiotów do nowych wymagań wskazują ten termin na 30 dni, jednocześnie przedmiotowe rozporządzenia ma wejść w życie po 14 dniach.

   Biorąc pod uwagę, że projekt w części wprowadza łagodniejsze wymagania niż obecnie obowiązujące, aby uniknąć problemów dla podmiotów rozpoczynających świadczenie usług objętych Rozporządzeniem, które byłyby zobowiązane poczynić inwestycje, które po 30 dniach od wejścia w życie przedmiotowych regulacji byłyby już nie wymagane, proponujemy rozważenie odpowiedniej modyfikacji w treści zapisów: skrócenie do 1 dnia terminu wejścia w życie rozporządzenia, ale jednocześnie wydłużenie do 60 dni terminu na dostosowanie do nowych wymagań. Dzięki takiej modyfikacji niezwłocznie będziemy korzystali z nowych, bardzo potrzebnych wymagań, a jednocześnie zapewnimy podmiotom odpowiedni czas na dostosowanie się do nowych wymagań.

Protokół z głosowania

Decyzją Wiceprzewodniczącego Rady głosowanie zostało przeprowadzone na posiedzeniu Rady do Spraw Cyfryzacji. Projekt uchwały nr 1 został poddany głosowaniu w dniu 19 lipca 2019 r. W głosowaniu wzięło udział 10 członków Rady, z czego oddano:

- 10 głosów „za" przyjęciem uchwały,
- 0 głosów „przeciw" oraz
- 0 głosów „wstrzymuję się".

Uchwała nr 1 Rady do Spraw Cyfryzacji została przyjęta w dniu 19 lipca 2019 roku w głosowaniu jawnym zwykłą większością głosów.

Szczegóły dotyczące głosowania przedstawia poniższa tabela.

Lp.	Imię	Nazwisko	Głos
1.	Joanna	Adamczyk	za
2.	Izabela	Albrycht	za
3.	Katarzyna	Chałubińska - Jentkiewicz	za
4.	Krzysztof	Głomb	za
5.	Agnieszka	Gryszczyńska	za
6.	Michał	Kanownik	za
7.	Tomasz	Łukawski	za
8.	Dariusz	Milka	za
9.	Włodzimierz	Schmidt	za
10.	Sebastian	Szymański	za

Przewodniczący Rady

Józef Orzeł
/-podpisano elektronicznie/