Konferencja Naukowa

POTRZEBY KOMPETENCYJNE W ZAKRESIE CYBERBEZPIECZEŃSTWA I ŁĄCZNOŚCI ELEKTRONICZNEJ W ŚWIETLE PLANOWANYCH ZMIAN W PRZEPISACH

2 października 2020 r.

Główne kierunki zmian w ustawie o krajowym systemie cyberbezpieczeństwa

Mariusz Busiło

Bącal Busiło LEGAL

Fundusze Europejskie Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Unia Europejska Europejski Fundusz Społeczny

Główne kierunki zmian w ustawie o krajowym systemie cyberbezpieczeństwa, mec. Mariusz Busiło

1. Identyfikacja i analiza problemu („Co nie działa i dlaczego?”)

2. Określenie celów („Jak powinno być? Co się powinno zmienić?”)

3. Określenie możliwych sposobów (opcji) realizacji celu („Jakie są sposoby poprawy danej sytuacji? Co się stanie gdy nie zrobisz nic?”)

4. Analiza kosztów i korzyści opcji działania („Ile to będzie kosztowało i jakie przyniesie korzyści? Kto straci a kto zyska?”)

5. Porównanie opcji działania i rekomendacja najlepszej z nich („Co rekomendujesz i dlaczego?”)

6. Określenie planu wdrażania i ewaluacji („Kiedy oczekujesz efektów i jak je zmierzysz?”)

7. Ewaluacja.

„WYTYCZNE do przeprowadzania oceny wpływu oraz konsultacji publicznych w ramach rządowego procesu legislacyjnego zgodnie z uchwałą nr 190 Rady Ministrów z 29 października 2013 r. – Regulamin pracy Rady Ministrów”

Zasada proporcjonalności – celowość i poprawność regulacji określa się w zależności od przedmiotu i zasięgu oddziaływania (skali kosztów i korzyści) danego rozwiązania (projektowanego aktu normatywnego); pogłębione analizy powinny być przeprowadzane dla projektów priorytetowych, o znacznych przewidywanych skutkach).

Zasada pomocniczości (subsydiarności) – każdy szczebel władzy powinien realizować tylko te zadania, które nie mogą być skutecznie zrealizowane przez szczebel niższy lub same jednostki działające w ramach społeczeństwa.

Zasada obiektywizmu – w trakcie przeprowadzanych analiz, a w szczególności przy wyborze rozwiązania, nie wolno dyskryminować żadnych podmiotów znajdujących się w tej samej sytuacji. Wyboru sposobu działania należy dokonywać po przeprowadzeniu, opartej na różnych źródłach, rzetelnej analizy.

Zasada przejrzystości i jawności – wymóg przeprowadzania konsultacji i przedstawiania ich wyników, informowania o źródłach informacji, a także prezentowania aktu prawnego na każdym etapie prac.

Główne kierunki zmian w ustawie o krajowym systemie cyberbezpieczeństwa, mec. Mariusz Busiło

Zmiany organizacyjne do KSC

(wynik 2 lat działania)

ISAC – centrum wymiany i analizy informacji na temat podatności, zagrożeń i incydentów funkcjonujące w celu wspierania podmiotów krajowego systemu cyberbezpieczeństwa (rejestr)

SOC – zespół pełniący funkcję operacyjnego centrum bezpieczeństwa w danym podmiocie

Zmiana obowiązków operatorów usług kluczowych (OUK):

„regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem poziomu krytyczności poszczególnych aktualizacji”
ZAMIAST „dbałości o aktualizację oprogramowania”
ORAZ
„ochrona dokumentów przed przypadkowym zniszczeniem, utratą, nieuprawnionym dostępem, niewłaściwym użyciem lub utratą integralności”
ZAMIAST „ochrony dokumentów przed niewłaściwym użyciem lub utratą integralności”

Obowiązek SOC dla OUK

Opcja SOC dla nie-OUK

Usprawnienie wymiany informacji za pośrednictwem wojewodów do samorządów

projekt wymaga w tym zakresie uporządkowania stosowanej terminologii i usunięcia nieznacznych niespójności

Główne kierunki zmian w ustawie o krajowym systemie cyberbezpieczeństwa, mec. Mariusz Busiło

Częściowa likwidacja sektorowej regulacji bezpieczeństwa i integralności sieci i usług telekomunikacyjnych / włączenie do KSC

Rozdział IVa uKSC zastępujący (?) Dział VIIa uPT oraz rozporządzenia z art. 175d (które wdrożyło 5G Toolbox i czeka na wejście w życie) oraz zaprojektowane przepisy uPKE (wdrożenie dyrektywy EKŁE)

niepewność regulacyjna, brak uzasadnienia takiej decyzji

powołanie CSIRT Telco / objęcie aktami władczymi Kolegium dsCB i Pełnomocnika Rządu dsCB.

istotne wątpliwości odnośnie proporcjonalności regulacji, przejrzystości procedury i skutków regulacji

poszerzenie obowiązków raportowych incydentów o CSIRT MON, CSIRT NASK lub CSIRT GOV.

„w zakresie niezbędnym do ich zadań" ?

Główne kierunki zmian w ustawie o krajowym systemie cyberbezpieczeństwa, mec. Mariusz Busiło

Oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa (art. 66a i nn)

„W sporządzania oceny przeprowadza się w szczególności”:

1) analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca

2) **prawdopodobieństwo, czy dostawca znajduje się pod wpływem państwa spoza UE lub NATO**, uwzględniającą a) **stopień i rodzaj powiązań** pomiędzy dostawcą i tym państwem, b) **prawodawstwo tego państwa** w zakresie ochrony praw obywatelskich i praw człowieka, c) prawodawstwo w zakresie ochrony danych osobowych, zwłaszcza tam gdzie nie ma porozumień w zakresie ochrony danych między UE i danym państwem, d) **strukturę własnościową dostawcy**, e) **zdolność ingerencji** tego państwa w swobodę działalności gospodarczej dostawcy

Do wniosku wystarczy IDENTYFIKACJA podmiotu oraz MOŻLIWYCH OBSZARÓW działalności, w których dostawca sprzętu lub oprogramowania MOŻE stanowić zagrożenie dla BEZPIECZEŃSTWA NARODOWEGO

3) liczbę i rodzaje oraz sposób i czas eliminowania wykrytych podatności i incydentów

4) stopień, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania

5) treść wydanych wcześniej rekomendacji, dotyczących sprzętu lub oprogramowania danego dostawcy [Badanie urządzenia informatycznego lub oprogramowania; rekomendacje dotyczące stosowania urządzeń informatycznych lub oprogramowania – przez CSIRT MON, CSIRT NASK lub CSIRT GOV]

Publikacja w Monitorze Polskim

Skutki Oceny Ryzyka Dostawcy

wysokie ryzyko, jeżeli dostawca oprogramowania stanowi poważne zagrożenie dla cyberbezpieczeństwa państwa i zmniejszenie poziomu tego ryzyka przez wdrożenie środków technicznych lub organizacyjnych nie jest możliwe	„odwołanie" do Kolegium w 14 dni od publikacji komunikatu. Kolegium rozpatruje w ciągu 2 miesięcy. Wniesienie odwołania nie wstrzymuje działań z art. 66b	1) Zakaz wprowadzania do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy; 2) Wycofanie z użytkowania sprzętu, oprogramowania i usług określonych w ocenie nie później niż 5 lat od dnia ogłoszenia komunikatu o ocenie
umiarkowane ryzyko, jeżeli dostawca stanowi poważne zagrożenie dla cyberbezpieczeństwa państwa a zmniejszenie poziomu tego ryzyka możliwe jest przez wdrożenie środków technicznych lub organizacyjnych	Dostawca może przedstawić Kolegium środki zaradcze i plan naprawczy. W przypadku akceptacji Kolegium może zmienić ocenę	1) Zakaz wprowadzania do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy; 2) Można kontynuować użytkowanie dotychczas posiadanych egzemplarzy sprzętu, oprogramowania oraz rodzaju i liczby usług
niskie ryzyko, jeżeli dostawca stanowi niewielkie zagrożenie dla cyberbezpieczeństwa państwa	Procedura oceny bez udziału stron i podmiotów zainteresowanych Brak kontroli sądowej	Utrzymanie? Aktualizacje? Usuwanie awarii?
brak zidentyfikowanego poziomu ryzyka, jeżeli nie stwierdzono zagrożenia dla cyberbezpieczeństwa państwa lub jego poziom jest znikomy		

Nowe uprawnienia Kolegium i Pełnomocnika

Pełnomocnik:

ostrzeżenie - w przypadku uzyskania informacji o zagrożeniu cyberbezpieczeństwa, która uprawdopodobni możliwość wystąpienia incydentu krytycznego

polecenie zabezpieczające - w przypadku wystąpienia incydentu krytycznego – po zatwierdzeniu przez Kolegium (w szczególnych bez)

Ostrzeżenie zawiera wskazanie określonego zachowania, wśród których jest także zakaz korzystania z określonego sprzętu lub oprogramowania oraz nakaz wprowadzenia reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL

Pełnomocnik wydaje polecenie zabezpieczające w drodze decyzji administracyjnej. Decyzja podlega natychmiastowemu wykonaniu.

Ostrzeżenia ogłasza się w Monitorze Polskim na okres do 2 lat z opcją przedłużenia na kolejne 2 lata.

Dziękuję za uwagę

Mariusz Busiło

Bącal, Busiło - Kancelaria prawna | Legal Advisors

M: +48 799 299 900 | @: m.busilo@telco.legal

Warszawa ul. Wspólna 70 | 1 piętro | 00-687 Warszawa

Poznań ul. Ratajczaka 44 | 61-728 Poznań