POLSKIE TOWARZYSTWO INFORMATYCZNE
Zarząd Główny, ul. Solec 38 lok. 103, 00-394 Warszawa, tel.: + 48 22 838 47 05, tel./fax: + 48 22 636 89 87, e-mail: pti@pti.org.pl, www.pti.org.pl

Stanowisko Polskiego Towarzystwa Informatycznego w sprawie projektu z dnia 23 kwietnia 2024 r. w sprawie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw

Niniejszym Polskie Towarzystwo Informatyczne przedstawia stanowisko w sprawie powyższej ustawy, dziękując jednocześnie za wyznaczenie 30 dniowego terminu, co miało istotne znaczenie dla odbycia konsultacji wewnętrznych, zważywszy na przypadający w tym okresie tzw. „długi weekend".

Poniżej przedstawiamy uwagi do poszczególnych zapisów projektu ustawy.

Uwagi do Art.1

1. W odniesieniu do art. 2 zmienianej ustawy w dodanym punkcie 3c) zawierającym definicję bezpieczeństwa systemów informatycznych proponuje się pozostawić jedynie trzy kardynalne atrybuty bezpieczeństwa (poufność, integralność, dostępność) wykreślając atrybut pomocniczy „autentyczność" jako zawierający się zgodnie z definicją ISO w atrybucie „integralność"

2. Art. 1 pkt 1) lit c) – w dodanej definicji 4b): *„dostawca sieci dostarczania treści – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która dostarcza sieci rozproszonych geograficznie serwerów służących zapewnieniu wysokiej i łatwej dostępności treści i usług cyfrowych lub ich szybkiego dostarczania na rzecz użytkowników internetu w imieniu dostawców treści i usług;"* jest niegramatyczna, przez co niezrozumiała

   Proponuje się zmianę: *„dostawca sieci dostarczania treści – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która dostarcza treści i usługi cyfrowe do sieci rozproszonych geograficznie serwerów służących zapewnieniu wysokiej i łatwej dostępności tych treści i usług lub ich szybkiego dostarczania na rzecz użytkowników internetu w imieniu dostawców treści i usług"*

3. Definicja 4e): *„dostawca usług chmurowych – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługi umożliwiające dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do ~~wspólnego~~ wykorzystywania przez wielu użytkowników"* jest nieprecyzyjna. Użytkownicy nie korzystają z zasobów „wspólnie". Sugeruje się wykreślić słowo „wspólnego"

4. Definicja 4h): *„dostawca usług zarządzanych – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługi związane z instalacją, eksploatacją lub konserwacją produktów ICT, usług ICT, procesów ICT lub systemów informacyjnych poprzez wsparcie lub aktywną administrację przeprowadzane u usługobiorcy lub zdalnie;"* zawiera kilka nieścisłości: 1) system informacyjny może składać się z produktów ICT lub procesów ICT; system(y) informacyjne realizuje(ą) usługi ICT; 2) „poprzez wsparcie lub aktywną administrację" – pojęcia

„wsparcie", a w szczególności „aktywna administracja" są niezrozumiale 3) „u usługobiorcy lub zdalnie" – zdalnie też jest „u usługobiorcy".

Sugeruje się następujące zmiany:

„dostawca usług zarządzanych – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługi związane z instalacją, eksploatacją lub konserwacją ~~produktów ICT, usług ICT, procesów ICT lub~~ systemów informacyjnych ~~poprzez wsparcie lub aktywną administrację~~ przeprowadzane u usługobiorcy, na miejscu lub zdalnie"

5. Definicja 4i) *„dostawca usług zarządzanych w zakresie cyberbezpieczeństwa – dostawca usług zarządzanych, który świadczy usługi związane z zarządzaniem ryzykiem w zakresie cyberbezpieczeństwa lub zapewnia pomoc dla tych działań;"* jest nieprecyzyjna i niekompletna

   Definicja zarządzanych usług bezpieczeństwa (managed security services) została wprowadzona do poprawki do Rozporządzenia EU 2019/881 (akt o cyberbezpieczeństwa w następującym brzmieniu: *„managed security service' means a service consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, including incident response, penetration testing, security audits and consultancy"*

   Dodatkowo, zarządzane usługi bezpieczeństwa nie są podzbiorem usług zarządzanych, stąd nie można zastosować „dostawca usług zarządzanych", bo reguła podstawienia definicji daje w wyniku nonsens.

   Sugeruje się powtórzenie definicji z poprawki do CSA w KSC:

   „dostawca zarządzanych usług bezpieczeństwa - osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługi polegające na realizacji lub wsparciu dla realizacji działań związanych z zarządzaniem ryzykiem w cyberbezpieczeństwie, w tym reakcja na incydenty, testy penetracyjne, audyty bezpieczeństwa oraz konsultacje"

6. lit i) Definicja: „11) *podatność – właściwość produktu ICT lub usługi ICT, które mogą być wykorzystane przez cyberzagrożenie;",* jest niepoprawna. Nie każda właściwość produktu lub usługi (a nawet ogromna większość) nie powoduje podatności

   Sugeruje się zmianę „właściwość" na „słabość" – jak od wielu lat definiuje się chociażby z normach związanych z ISO/IEC 27001

7. lit i) Definicja 11e): „potencjalne zdarzenie dla cyberbezpieczeństwa – zdarzenie, które może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych; – definicja w konflikcie z definicją incydentu i po prostu niepotrzebna, wystarczy użyć „potencjalny incydent" co oznacza: „potencjalne zdarzenie, które ma, lub może mieć niekorzystny wpływ na system informacyjny"

   Sugeruje się wykreślenie definicji

8. Pkt 12, ust. 2: „2. *Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem*

informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO 22301." Przepis jest nieprecyzyjny. Czy ma być to deklaracja? Potwierdzeniem spełnienia wymagań jest certyfikat zgodności dla poprawnie zdefiniowanego zakresu systemu zarządzania bezpieczeństwem informacji, czyli w odniesieniu do KSC, usług świadczonych przez podmiot kluczowy lub podmiot ważny, z wymaganiami norm.

Sugeruje się następującą zmianę:

„2. *Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, zgodny z wymaganiami ~~z uwzględnieniem wymagań~~ określonymi w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO 22301, co potwierdzają odpowiednie certyfikaty wydane przez akredytowane jednostki certyfikujące lub deklaracja własna podmiotu."*

9. W dodanym punkcie 11b) zawierającym definicję podmiotu publicznego wskazano błędnie tytuł ustawy („ustawa w sektorze administracji publicznej" nie istnieje). Należy wskazać prawidłowy tytuł ustawy którą Autor miał na myśli

10. Zmienione brzmienie art. 8 w ust. 1 w punkcie 2) podpunkt f) zawiera wymóg objęcia systemu informatycznego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym. Proponuje się doprecyzowane wymogu monitorowania przez dodanie wyrazów „*pod kątem zagrożeń cyberbezpieczeństwa*", gdyż praktyka audytowa wykazała, że niektóre podmioty za spełniony wymóg uważają prowadzenie monitorowania wyłącznie pod kątem ich standardowej aktywności (obciążenie procesorów, zajętość pamięci RAM, zajętość pamięci zewnętrznych, ruch sieciowy etc.)

11. W zmienionym brzmieniu art. 8 w ust. 1 w punkcie 5 podpunkt a) proponuje się wykreślić atrybut pomocniczy „autentyczność" (patrz uwaga nr 1)

12. W zmienionym brzmieniu art. 8 ust. 2 wskazującym na wymagania określone w normach błędnie podano tytuł (organizację) przy których norma jest akredytowana. Dotyczy to normy PN-EN ISO 22301 (norma nie jest akredytowana przy IEC). W obecnym brzmieniu art.10 ust. 3 pkt 3) podano prawidłową nazwę normy jako PN-EN ISO 22301

13. W dodanym artykule 8c pkt 3 należy doprecyzować odpowiedzialność kierownika podmiotu kluczowego, także w przypadku, gdy wszystkie obowiązki wynikające ze zmienionej ustawy zostały powierzone innej osobie za jej zgodą (wersja w projekcie wskazuje jedynie na przekazanie „*niektórych obowiązków*")

14. Art. 2 pkt 14 podpunkt b) zmienianej ustawy otrzymuje brzmienie:

b) urządzenie lub grupę połączonych urządzeń elektrycznych lub elektronicznych i oprogramowania zaprogramowanych w celu przetwarzania danych – wraz z danymi przetwarzanymi w postaci elektronicznej;"

Określenie „oprogramowania zaprogramowanego" stanowi tautologię. Całość zapisu jest niezrozumiała. Zaprogramowane (czyli posiadające zdolność do wykonania sekwencji działań zależnych od poprzedniego stanu – teoria automatów – maszyna Turinga) może być dowolne urządzenie posiadające zdolność wykonywania kolejnych działań, zależnych, lub

niezależnych od poprzedniego stanu. W dokumencie „UZASADNIENIE" podano: „– „*W ten sposób projektodawca chce przeciąć wątpliwości co do tego czy systemy OT mieszczą się w ramach obecnej definicji systemu informacyjnego czy nie".* Wskazać należy, że taka wątpliwość nigdy nie istniała, bo każde urządzenie elektromechaniczne spełniające warunki wskazane w teorii automatów jest systemem informatycznym, gdyż jego działanie zależy od przetwarzanej informacji

Proponuje się zapis: *b) teleinformatyczny system sterujący lub monitorujący czasu rzeczywistego;* Biorąc pod uwagę, że przedmiotem regulacji są urządzenia elektryczne (elektroniczne stanowią ich odmianę- na ogół niskonapięciową, poza elementami mocy – tyrystory, triaki, czy tranzystory wysokonapięciowe), zapis – *wraz z danymi przetwarzanymi w postaci elektrycznej* – jest niepotrzebny

15. Uchylenie art. 14 zmienianej ustawy tworzy niepewność co do obowiązku utworzenia własnych struktur odpowiedzialnych za cyberbezpieczeństwo, lub możliwości powierzenia tych zadań podmiotowi zewnętrznemu. Szczególne znaczenie może to mieć dla podmiotów publicznych których działania nie mogą opierać się na zasadzie „co nie jest zakazane jest dozwolone"

16. W proponowanym brzmieniu art. 15 pkt a) ust.1zmienianej ustawy nakłada się obowiązek przeprowadzania regularnego audytu (co 2 lata) zarówno na podmioty kluczowe jak i podmioty ważne, co wykracza poza wytyczne dyrektywy NIS 2 która nakłada obowiązek wykonywania takich (regularnych) audytów jedynie na podmioty kluczowe. Zważywszy na oszacowaną obecnie liczbę podmiotów kluczowych i ważnych (ok. 38 tys.) wykonanie tego obowiązku przez oba typy wskazanych podmiotów jest wątpliwe. Proponuje się sformułowanie: *Podmiot kluczowy ma obowiązek zapewnić przeprowadzenie, na własny koszt, co najmniej raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi, zwanego dalej „audytem*"

17. W art. 15 ust. 2 pkt 2 podpunkt b) i c) zmienianej ustawy pozostawiono możliwość wykonywania audytów przez osoby nie posiadające certyfikatów uprawniających do wykonywania audytów. Dotychczasowa praktyka dowiodła, że często osoby te nie potrafią należycie ocenić bezpieczeństwa ocenianego podmiotu. Jako minimalny wymóg proponuje się w miejsce podpunktów b) i c) wstawić punkt b) *co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa uzyskaną po otrzymaniu certyfikatu audytora wewnętrznego w zakresie normy PN-EN ISO/IEC 27001*

18. W art. 26 w dodanym ust. 2b należy doprecyzować termin w którym zgoda wyrażona ustnie ma być udokumentowana

19. W art.26 w nowym brzmieniu punktu 12 należy uzupełnić w punkcie d) brakujący nawias oraz dodać określenie „*mających znaczenie*" przed wyrażeniem „*dla cyberbezpieczeństwa*"

20. W dodanym rozdziale 6a **Ocena bezpieczeństwa** Art. 36b ust. 4 wydaje się zbędny w związku z brzmieniem Art. 296b § 1a Kodeksu Karnego, gdyż cel tam wymieniony w całości pokrywa się z celem w jakim mogą działać wymienione CSIRT-y (działanie w celu

zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstw)

21. W art. 56 w dodanym ust. 3 wskazany wymóg tłumaczenia dokumentacji przez podmiot kontrolowany należy doprecyzować w sposób następujący: „*Tłumaczenie powinno być wykonane przez tłumacza przysięgłego*" ze względu na konieczność wiernego przetłumaczenia takiej dokumentacji

22. W dodanym do zmienianej ustawy art. 67b ust.1określającym uprawnienie Ministra właściwego ds. informatyzacji do wszczęcia postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, proponuje się ograniczyć zakres podmiotów w stosunku do których decyzja taka może być wydana jedynie do podmiotów kluczowych. Przesłanką do takiej zmiany jest zarówno szacowana liczba podmiotów ważnych która mogłaby zostać objęta skutkami takiej decyzji, jak i możliwość jej faktycznego wykonania przez te podmioty

Proponowany zapis art. 67b ust.1 p 1): „*podmioty kluczowe, z wyłączeniem podsektora komunikacji elektronicznej lub*"

23. Pkt 70, art. 67b, ust 11 ppkt 4): „*liczby i rodzajów wykrytych podatności i incydentów dotyczących typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;"* – kryterium jest nieprecyzyjne; wykryte przez kogo? W jakim okresie? – zapis wymaga doprecyzowania

24. Pkt 70, art. 67b, ust 11 ppkt 5): „*trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów,"* – kryterium jest nieprecyzyjne. Co oznacza „trybu i zakresu"? jaki tryb jest akceptowalny? Czy jeśli wiodący europejski dostawca sprzętu telekomunikacyjnego ma 6000 dostawców w łańcuchu dostaw, to należy uznać, że sprawuje wystarczający nadzór? A nie będzie on wystarczający, jeśli dotyczyłoby to dostawcy azjatyckiego? Kryterium jest skrajnie nieprecyzyjne. Należy rozważyć jego wykreślenie

25. Pkt 70, art. 67g, ust. 1 „*Minister właściwy do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego może, w drodze decyzji, wydać polecenie zabezpieczające*" – uczestnictwo Ministra w obsłudze incydentu krytycznego jest wątpliwe – jedyną przyczyną takiego stanu rzeczy byłaby procedura eskalacji, kiedy CSIRT-y nie dają rady obsłużyć incydentu z uwagi na skalę lub powagę konsekwencji, to powinno być opisane jako czynnik uruchamiający działania ekstraordynaryjne Ministra; całość tego przepisu jest niedopracowana i powinna powrócić na ścieżkę uzgodnień technicznych z ekspertami. Poniżej przedstawiamy dalsze zastrzeżenia do konkretnych punktów trybu wprowadzenia oraz zakresu „polecenia zabezpieczającego"

26. Pkt 70, art. 67g, ust. 5 „*Przed wydaniem polecenia zabezpieczającego minister właściwy do spraw informatyzacji przeprowadza we współpracy z Zespołem, o którym mowa w art. 35 ust. 3, analizę obejmującą* (...)" – to powinna być określona procedura eskalacji, a czynnik uruchomienia procedury powinien wynikać z prac CSIRT-ów przy obsłudze incydentu krytycznego

27. Pkt 70, art. 67g, ust 10 ppkt 3) dot. „określonego zachowania": *„nakaz zastosowania określonej poprawki bezpieczeństwa w produkcie ICT, procesie ICT lub usłudze ICT posiadającym daną podatność*;" – z analizy wykonanej przez dany podmiot może wynikać, że w danej konfiguracji, w danym systemie poprawki NIE DA się wprowadzić; z tego względu proponuje się wprowadzić uzupełnienie:

„w wypadku, gdy z przyczyn technicznych, organizacyjnych lub biznesowych tej poprawki bezpieczeństwa nie można wprowadzić, podmiot będący stroną postępowania zabezpieczającego przedstawia swoje stanowisko, wraz z uzasadnieniem, które jest brane pod uwagę przez ministra właściwego do spraw informatyzacji."

28. Pkt 70, art. 67g, ust 10 ppkt 4) dot. „określonego zachowania": *„nakaz szczególnej konfiguracji produktu ICT, usługi ICT lub procesu ICT, zabezpieczającej przed wykorzystaniem określonej podatności*;" - z analizy wykonanej przez dany podmiot może wynikać, że wskazanej konfiguracji w danym konkretnym systemie NIE DA się wprowadzić; z tego względu proponuje się wprowadzić uzupełnienie:

„w wypadku, gdy z przyczyn technicznych, organizacyjnych lub biznesowych nakazywanej konfiguracji nie można zastosować, podmiot będący stroną postępowania zabezpieczającego przedstawia swoje stanowisko, wraz z uzasadnieniem, które jest brane pod uwagę przez ministra właściwego do spraw informatyzacji."

29. Pkt 70, art. 67g, ust 10 ppkt 5) dot. „określonego zachowania": *„nakaz wzmożonego monitorowania zachowania systemu"* – jest to sformułowanie nieprecyzyjne; co Autor ma na myśli, nakazując „wzmożone monitorowanie"? Zważyć należy, że działające obecnie systemy monitorowania bezpieczeństwa klasy SIEM lub SOAR działają w oparciu o rozwiązania sprzętowo-programowe których zachowanie (wyświetlanie alertów personelowi monitorującemu – SOC) bazuje na predefiniowanych regułach korelujących określone zdarzenia w monitorowanym systemie. Wzmożone monitorowanie wymagałoby zmiany tych reguł polegające na wykrywanie szerszej klasy zdarzeń, niekoniecznie z pozytywnym skutkiem dla faktycznego bezpieczeństwa, na skutek wywoływania fałszywych alertów tzw. False Positive. Prowadzi to najczęściej do przemęczenia personelu i może spowodować skutek odwrotny do zamierzonego.

Potrzebne jest wyjaśnienie, o jakie działanie tu chodzi. Jeśli nie można tego wyjaśnić, to proponuje się skreślić ten podpunkt.

30. Pkt 70, art. 67g, ust 10 ppkt 6) dot. „określonego zachowania": *zakaz korzystania z określonego produktu ICT, usługi ICT lub procesu ICT, które posiada podatność, która przyczyniła się do zaistnienia incydentu krytycznego*;" - z analizy wykonanej przez dany podmiot może wynikać, że danego elementu systemu NIE DA się usunąć; z tego względu proponuje się wprowadzić uzupełnienie:

„w wypadku, gdy z przyczyn technicznych, organizacyjnych lub biznesowych zakazu nie można zastosować, podmiot będący stroną postępowania zabezpieczającego przedstawia swoje stanowisko, wraz z uzasadnieniem, które jest brane pod uwagę przez ministra właściwego do spraw informatyzacji."

31. Pkt 70, art. 67g, ust 10 ppkt 9) i 10) dot. *„9) nakaz zabezpieczenia określonych informacji, w tym dzienników systemowych; 10) nakaz wytworzenia obrazów stanu określonych urządzeń zainfekowanych złośliwym oprogramowaniem*." – takie informacje zbiera się w trakcie trwania incydentu od samego początku, stąd mechanizm polecenia zabezpieczającego może być mało skuteczny – często już jest za późno na pozyskanie takich informacji; sugeruje się dodać na końcu ppkt 9 oraz 10) odpowiednio: „o ile takie informacje są możliwe do pozyskania"

32. Pkt 70, art. 67g, ust 11 „11. *Wskazanie obowiązku określonego zachowania, o którym mowa w ust. 9 pkt 2, następuje z uwzględnieniem środków adekwatnych, w szczególności w świetle analizy, o której mowa w ust. 5."* – co oznacza „środki adekwatne"? Adekwatne do czego? Wskazanie powinno być dość precyzyjne, ponieważ polecenie zabezpieczające zawiera same zakazy i nakazy, a środki adekwatne mogą sugerować ominięcie tych zakazów lub nakazów. Proponuje się zmianę tego zapisu na: *Wskazanie obowiązku określonego zachowania, o którym mowa w ust. 9 pkt 2, następuje z uwzględnieniem dobrych praktyk, w szczególności w świetle analizy, o której mowa w ust. 5*" lub skreślenie tego ustępu

33. Pkt 73, art. 72b, ust. 2: ppkt 2) *„cele krajowych środków i działań służących w zakresie gotowości;"* – to zdanie nie ma żadnej treści; prośba o analizę, co Autor miał na myśli

34. Pkt 73, art. 72b, ust. 2 ppkt 3): *„procedury zarządzania kryzysowego w cyberprzestrzeni, w tym ich włączenie do ogólnych krajowych ram zarządzania kryzysowego, oraz kanały wymiany informacji*;" – do przemyślenia przez Autorów ustawy powiązanie mechanizmu „polecenia zabezpieczającego", o którym mowa w art. 67g z procedurą eskalacji, która zwykle wpada w zarządzanie kryzysowe

35. Pkt 74, art. 73a), ust 1 ppkt 2) *„nie przeprowadził systematycznego szacowania ryzyka lub nie zarządził ryzykiem wystąpienia incydentu,* o których mowa w art. 8 ust. 1 pkt 1;" – zdanie niepoprawne gramatycznie, nie można trybu dokonanego używać do czynności systematycznych lub o charakterze ciągłym; proponuje się zmianę: nie przeprowadzał (..) lub nie zarządzał (..)

Uwagi do Art.2

1. W zmienianej ustawie z dnia 21 marca 1991 o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej w ustępie 2a, stosownie do zmian proponowanych w Art.1 omawianej ustawy (pkt. 3 przedkładanych uwag) proponuje się usunięcie słowa „wspólnego".

Uwagi do Art.3

2. W Art.3 omawianej ustawy zmieniającej ustawę z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa w dodanym art. 299i w końcu akapitu należy uzupełnić enumeratywnie wymieniane w nawiasie pozycje (aktualny zapis – Dz. U. z 2023 r. poz. 913,1703 i …).

Uwagi do ZAŁĄCZNIKA NR 1 PODMIOTY KLUCZOWE

1. Podmioty zajmujące się produkcją, przetwarzaniem i dystrybucją żywności zostały w projekcie ustawy sklasyfikowane jako podmioty kluczowe. Zważyć należy, że dyrektywa

NIS 2 klasyfikuje te podmioty jako podmioty ważne. Podniesienie rangi tych podmiotów stanowi tzw. nadregulację i spowoduje zbędne obciążenie dla tych podmiotów i systemu nadzoru. Sugeruje się przeniesienie podmiotów tego sektora do ZAŁĄCZNIKA NR 2 PODMIOTY WAŻNE.

2. Podmioty zajmujące się produkcją, wytwarzaniem i dystrybucją chemikaliów zostały w projekcie ustawy sklasyfikowane jako podmioty kluczowe. Zważyć należy, że dyrektywa NIS 2 klasyfikuje te podmioty jako podmioty ważne. Podniesienie rangi tych podmiotów stanowi tzw. nadregulację i spowoduje zbędne obciążenie dla tych podmiotów i systemu nadzoru. Sugeruje się przeniesienie podmiotów tego sektora do ZAŁĄCZNIKA NR 2 PODMIOTY WAŻNE.

3. Podmioty zajmujące się produkcją (wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro, komputerów, wyrobów elektronicznych i optycznych, urządzeń elektrycznych, maszyn i urządzeń, gdzie indziej niesklasyfikowana, pojazdów samochodowych, przyczep i naczep, pozostałego sprzętu transportowego) zostały w projekcie ustawy sklasyfikowane jako podmioty kluczowe. Zważyć należy, że dyrektywa NIS 2 klasyfikuje te podmioty jako podmioty ważne. Podniesienie rangi tych podmiotów stanowi tzw. nadregulację i spowoduje zbędne obciążenie dla tych podmiotów i systemu nadzoru. Sugeruje się przeniesienie podmiotów tego sektora do ZAŁĄCZNIKA NR 2 PODMIOTY WAŻNE.

Uwagi do dokumentu „UZASADNIENIE”

a. Str. 73, cyt. *„Zmitygowanie ryzyka sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka nie jest także możliwe poprzez obowiązkową certyfikację sprzętu lub oprogramowania. Standardy certyfikacyjne nie zawsze będą w stanie pomóc przy wykryciu ukrytych podatności, zwłaszcza jeśli sam producent chce je ukryć. Ponadto standardy te są znane samemu producentowi, który może to wykorzystać*”.

Powyższy akapit jest wielokrotnie nieprawdziwy.

1. Zgodnie z art. 67b ust.: *12. Sporządzając opinię, o której mowa w ust. 10 zdanie pierwsze, Kolegium uwzględnia:*

1) certyfikaty wydane dla produktów ICT, usług ICT lub procesów ICT, wydane lub uznawane w państwach członkowskich Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, w szczególności certyfikaty wydane w ramach europejskich programów certyfikacji cyberbezpieczeństwa”.

Oznacza to, że czynnikiem ryzyka, który bierze pod uwagę Kolegium, jest obecność lub brak uznawanych certyfikatów. Obowiązkowa certyfikacja niewątpliwie wpływa na poziom ryzyka związanego z użyciem produktów/usług od „dostawcy wysokiego ryzyka.”

2. Następnie, w przepisach dot. opracowywania strategii (art. 69) ust. 2: *2) przy opracowywaniu strategii uwzględnia się: 2) Rozwiązania dotyczące uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów ICT i usług ICT oraz specyfikacji tych wymogów na potrzeby takich zamówień, w tym w odniesieniu do certyfikacji cyberbezpieczeństwa (..)*”

3. Kolejno, należy podkreślić, że nie ma czegoś takiego jak „standardy certyfikacji”. Są normy referencyjne, które określają, w jaki sposób przeprowadzić analizę podatności. Realizując wymagania normy ewaluacyjnej, podatności mogą być wykrywane. Nikt nie może zagwarantować, że zostaną wykryte wszystkie podatności – nie ma takiej uniwersalnej magicznej formuły.

4. Wreszcie, niezależnie od tego, że „standardy certyfikacji” nie istnieją, to znajomość ich przez dostawcę nie ma żadnego znaczenia dla procesu oceny bezpieczeństwa. Dostawca nie ma wpływu, w jaki sposób ewaluatorzy prowadzą analizę podatności. Wynik zależy od umiejętności ewaluatorów, a nie od tego, czy dostawca coś ukrywa albo nie.

Z powyższych względów, sugeruje się wykreślenie wskazanego akapitu.

Na tym stanowisko zakończono.

Uwagi zostały opracowane przez Zespół w składzie:

1. Elżbieta Andrukiewicz – ela@andrukiewicz.pl
2. Jakub Kulesza – jakub@kulesza.pl
3. Wacław Iszkowski – waclaw@iszkowski.eu
4. Marek Ujejski – marek.ujejski@pti.org.pl

W ewaluacji końcowej udział wzięli:

1. Adrian Kapczyński – adrian.kapczynski@pti.org.pl
2. Rafał Kołodziejczyk – rafal.kolodziejczyk@pti.org.pl
3. Danuta Morańska – danuta.moranska@pti.org.pl
4. Robert Ostrowski – robert.r.ostrowski@gmail.com
5. Monika Słomkowska – monika.slomkowska@gmail.com
6. Beata Ostrowska – beata.ostrowska@pti.org.pl

Prezes Polskiego Towarzystwa Informatycznego

Dokument podpisany przez Wiesław Paluszyński
Data: 2024.05.24 10:37:58 CEST

Wiesław Paluszyński


POLSKIE TOWARZYSTWO INFORMATYCZNE