CYBERPOLICY

Review

Biuletyn NASK

Strategia. Policy. Rekomendacje.

NASK

Biuletyn NASK

Strategia. Policy. Rekomendacje.

Nr 1/ lipiec 2017

Redakcja: Magdalena Wrzosek

Czym jest Cyber Policy Review?

Państwowy Instytut Badawczy NASK od dawna prowadzi działania zmierzające do podnoszenia bezpieczeństwa teleinformatycznego w Polsce. Od 1996 roku w strukturze Instytutu działa zespół CERT Polska, pierwszy w Polsce zespół reagowania na incydenty. Na bazie doświadczeń CERT Polska, w lipcu 2016 roku, utworzone zostało NC Cyber. Jest to pion w strukturze Państwowego Instytutu Badawczego NASK, którego misją jest dbanie o bezpieczeństwo cyberprzestrzeni Rzeczypospolitej Polskiej. Dzięki nabytym doświadczeniom i wciąż rozwijanym kompetencjom NC Cyber przyczynia się do wzrostu bezpieczeństwa cyberprzestrzeni RP i prowadzi współpracę międzynarodową w tym zakresie.

Działalność PIB NASK dotyczy poziomu operacyjnego (CERT Polska oraz działające w trybie dwudziestoczterogodzinnym Centrum Operacyjne), oraz działania na poziomie strategicznym i tzw. policy, które koncertują się na prawnej i strategicznej analizie inicjatyw związanych z cyberbezpieczeństwem i gospodarką, oraz stymulowaniem współpracy pomiędzy administracją, a sektorem prywatnym. Częścią tych działań jest „Cyber Policy Review" – biuletyn, którego zadaniem jest przybliżenie kwestii związanych z najnowszymi regulacjami prawnymi i inicjatywami strategicznymi związanymi z cyberbezpieczeństwem.

Wyrażam nadzieję, że jego pierwszy numer będzie dla Państwa interesujący.

dr inż. Wojciech Kamieniecki, Dyrektor Państwowego Instytutu Badawczego NASK

Spis treści

Maciej Bednarek
Magdalena Wrzosek

Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022

9 maja 2017 r. rząd przyjął uchwałę w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022. (Uchwała Rady Ministrów nr 52/2017)[1]. W przeciwieństwie do Założeń, opublikowanych w lutym 2016 roku, dokument ten został opracowany przez grupę ekspertów w skład której weszli przedstawiciele resortów: cyfryzacji, obrony narodowej, spraw wewnętrznych i administracji oraz funkcjonariusze i przedstawiciele Agencji Bezpieczeństwa Wewnętrznego, Rządowego Centrum Bezpieczeństwa, Biura Bezpieczeństwa Narodowego i PIB NASK. Dzięki temu wypracowany dokument ma charakter interdyscyplinarny i odnosi się do szerokiego spektrum potrzeb w dziedzinie cyberbezpieczeństwa. Ponieważ Krajowe Ramy przyjęte zostały, jako uchwała Rady Ministrów, obowiązują tylko administrację rządową.

Co za tym idzie, stanowią zbiór deklaracji i założeń, jakimi kierował się będzie rząd przy tworzeniu zapowiadanej ustawy o krajowym systemie cyberbezpieczeństwa. Krajowe Ramy zastąpiły Politykę Ochrony Cyberprzestrzeni RP, opracowaną przez ówczesne Ministerstwo Administracji i Cyfryzacji, przyjętą przez rząd w czerwcu 2013 roku.

Wizja rządu jest następująca:

W roku 2022 Polska będzie krajem bardziej odpornym na ataki i zagrożenia płynące z cyberprzestrzeni. Dzięki synergii działań wewnętrznych i międzynarodowych cyberprzestrzeń RP stanowić będzie bezpieczne środowisko umożliwiające realizowanie wszystkich funkcji państwa i pozwalać na pełne wykorzystywanie potencjału gospodarki cyfrowej, przy równoczesnym poszanowaniu praw i wolności obywateli.

Głównym celem *Krajowych Ram* jest *zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych.* Poza tym wyodrębnione zostały też cztery cele szczegółowe, wskazujące na potrzeby, jakie wynikają z rozbudowy krajowego systemu cyberbezpieczeństwa:

1. Osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa
2. Wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom.
3. Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni.
4. Zbudowanie silnej pozycji międzynarodowej Polski w obszarze cyberbezpieczeństwa.

Realizacja tych celów będzie związana ze zmianami prawnymi oraz udoskonaleniem struktury systemu cyberbezpieczeństwa poprzez jasny podział kompetencji, który zwiększy efektywność współdziałania podmiotów odpowiedzialnych za bezpieczeństwo sieci. Wiązać się to będzie również ze stworzeniem i wdrożeniem systemu zarządzania ryzykiem teleinformatycznym w skali kraju. Duży nacisk położony został także na ochronę infrastruktury krytycznej usług kluczowych i cyfrowych, zwalczanie cyberprzestępczości i cyberterroryzmu, a także uzyskania zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni. Ważnym elementem dokumentu jest także budowanie kompetencji w zakresie cyberbezpieczeństwa – rozbudowana zasobów przemysłowych i technologicznych, budowanie partnerstw publiczno – prywatnych, stymulo-

[1] *Dokument jest dostępny pod adresem: http://m.mc.gov.pl/files/krajowe_ramy_polityki_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf*

wanie badań i rozwoju, a także edukacja w zakresie cyberbezpieczeństwa.

Ponieważ *Krajowe Ramy* mają charakter ogólnych celów, wytycznych i deklaracji, grupa ekspertów pracuje obecnie nad Planem działań – dokumentem który zoperacjonalizuje te cele.

Krajowe Ramy Polityki Cyberbezpieczeństwa zostały ustanowione na okres pięciu lat. **Funkcję koordynatora podczas procesu wdrażania tej uchwały będzie sprawował minister właściwy do spraw informatyzacji.** Po upływie dwóch lat od wprowadzenia uchwały, a następnie w czwartym roku jej obowiązywania planowane jest wykonanie przeglądów oraz dokonanie oceny efektów, jakie dokument do tej pory wprowadzi. Rezultaty będą przedstawione Radzie Ministrów, a minister właściwy do spraw informatyzacji będzie zobowiązany do opracowania propozycji działań korygujących lub projektu dokumentu na okres kolejnych pięciu lat.

Rozmowa z Minister Cyfryzacji, Anną Streżyńską, na temat Krajowych Ram Polityki Cyberbezpieczeństwa.

Priorytetem jest stworzenie krajowego systemu cyberbezpieczeństwa, zarówno w warstwie prawnej, organizacyjnej jak i technologicznej. Przed nami więc ustawa o krajowym systemie cyberbezpieczeństwa, zbudowanie systemu łączności oraz systemu bieżącego zarządzania bezpieczeństwem w cyberprzestrzeni.

Redakcja (R): Proces powstawania krajowego dokumentu strategicznego w dziedzinie bezpieczeństwa cyberprzestrzeni trwał wiele miesięcy. Ostatecznie został on wypracowany w zespole międzyresortowym. Kto brał udział w pracach nad tym dokumentem i czy ta formuła współpracy zostanie utrzymana w przyszłości?

Minister Anna Streżyńska (MAS): Proces powstawania Krajowych Ram Polityki Cyberbezpieczeństwa na lata 2017-2022 nie był łatwy. Wiele mówiło się przy tej okazji na temat „docierania się" między resortami. Ostatecznie dokument został przyjęty, a został wypracowany w zespole, w którym znaleźli się eksperci ze wszystkich resortów. Są to zapisy kompromisowe i uwzględniające wszystkie punkty widzenia. W zespole pracowali prawnicy, inżynierowe i specjaliści od kreowania polityki państwa. Oprócz przedstawicieli MC w proces zaangażowani byli przedstawiciele MON, w tym SKW, MSWiA, w tym Policji, ABW, RCB, BBN, MSZ oraz NASK. Taka formuła współpracy jest utrzymywana i dotyczy także prac nad Planem działania na rzecz wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa. Zespół został rozszerzony o przedstawicieli MR, MNiSW oraz MEN. W podobnym składzie prowadzone są zresztą również konsultacje przepisów ustawy o krajowym systemie cyberbezpieczeństwa.

R: Jak MC ocenia rolę Krajowych Ram w całej sekwencji zadań na rzecz dosko-

nalenia systemu ochrony na poziomie krajowym i jakie będą kolejne kroki oraz działania na tej drodze? Jak wpisuje się ten dokument w strategiczne programy ministra cyfryzacji?

MAS: Strategia cyberbezpieczeństwa to dokument o strategicznym znaczeniu. Nakreśla kierunki działań w zakresie zapewnienia bezpieczeństwa korzystania z cyberprzestrzeni. Teraz należy ten dokument wdrożyć i to na kilku poziomach: prawnym, organizacyjnym i technologicznym. Wszystko to ma zapewnić właściwy poziom bezpieczeństwa w cyberprzestrzeni. Szczególnie dla usług udostępnianych dla obywateli.

R: Jaką rolę będzie odgrywało MC w procesie realizacji krajowych ram?

MAS: MC występować będzie w podwójnej roli. Zgodnie z zapisami uchwały rządu, która wprowadza Strategię cyberbezpieczeństwa, MC pełni rolę koordynatora działań wdrażających. We współpracy z innymi ministrami, kierownikami urzędów centralnych oraz Dyrektorem RCB musimy teraz opracować plan wdrożenia Strategii cyberbezpieczeństwa. Odpowiadamy za to. Z drugiej strony będziemy jednak realizować znaczącą liczbę działań.

R: Jakie są główne priorytety działań wynikające z krajowych ram?

MAS: Priorytetem jest stworzenie krajowego systemu cyberbezpieczeństwa, zarówno w warstwie prawnej, organizacyjnej jak i technologicznej. Przed nami więc ustawa o krajowym systemie cyberbezpieczeństwa, zbudowanie systemu łączności oraz systemu bieżącego zarządzania bezpieczeństwem w cyberprzestrzeni. Obecnie NASK uzyskał grant NCBiR na opracowanie Narodowej Platformy Cyberbezpieczeństwa, która jest elementem wspomnianego systemu zarządzania bezpieczeństwem. Niewątpliwie głównym zadaniem po stronie MC jest przygotowanie projektu ustawy o krajowym systemie cyberbezpieczeństwa. Zakładamy, że w połowie sierpnia projekt ustawy zostanie skierowany do uzgodnień międzyresortowych i konsultacji społecznych. Zamknięcie procesu legislacyjnego po stronie rządowej i przekazanie projektu Marszałkowi Sejmu, powinno nastąpić z końcem bieżącego roku.

R: Czy można powiedzieć, w jaki sposób będzie finansowane wdrażanie Krajowych Ram? Jak ten proces będzie przebiegał?

MAS: Przedsięwzięcia z zakresu wdrażania strategii, które mają charakter działań ciągłych, będą zasadniczo finansowane w ramach planów finansowych podmiotu realizującego dane działanie, czyli po prostu przez poszczególnych ministrów. W odniesieniu do zadań o charakterze projektowym, których realizacja ma się rozpocząć w roku 2018, MC wystąpiło z wnioskiem o utworzenie celowej rezerwy budżetowej. Źródłem finansowania będą też konkursy ogłaszane przez NCBiR, a także z fundusze POPC.

R: Krajowe ramy przewidują opracowanie w ciągu 6 miesięcy planu działań na rzecz wdrożenia krajowych ram. Jaka jest funkcja tego dokumentu i jak przebiegają obecnie prace nad nim?

MAS: Plan działań jest dokumentem wykonawczym Strategii cyberbezpieczeństwa. Trwają prace międzyresortowej grupy roboczej, która ma za zadanie opracowanie Planu. W grupie roboczej uzgodniono już, jakie działania należy podjąć, by uzyskać szczegółowe cele Strategii. Następnym etapem będzie zadeklarowanie się podmiotów wiodących w zakresie określonego działania, co do realizacji konkretnych zadań, z określeniem celu szczegółowego w ramach Strategii. Potrzebne jest dopracowanie wszystkich szczegółów, harmonogramów poszczególnych działań, a także wyliczenie szacunkowych kosztów. Zgodnie z postanowieniem uchwały Plan działań wdrażających powinien być gotowy nie później niż do 27 października 2017 r. W chwili obecnej MC oczekuje na wkłady do tego dokumentu od urzędów będących podmiotami wiodącymi w poszczególnych działaniach. Powinniśmy je mieć do 1 sierpnia 2017 r., co z kolei umożliwi opracowanie Planu działań w zakładanym terminie.

R: Dyrektywa NIS zakłada przyjęcie krajowej strategii bezpieczeństwa sieci i informacji. Czy w związku z tym dokument KRPC, który został przyjęty w drodze uchwały RM zostanie w przyszłości w inny sposób umocowany w polskim prawie by mógł dotyczyć wszystkich sektorów dyrektywy?

MAS: Według opracowywanego projektu ustawy implementującej NIS do polskiego systemu prawnego, strategia pozostanie uchwałą Rady Ministrów. Będzie to deklaracja polityczna Rządu w zakresie działań dotyczących cyberbezpieczeństwa. Odziaływanie prawne na sektory wymienione w NIS, ale też na pewne sektory, które w NIS nie są wymienione, co dyrektywa pod pewnymi warunkami dopuszcza, odbywać się będzie poprzez przepisy prawa. W szczególności przez przepisy projektowanej ustawy o krajowym systemie cyberbezpieczeństwa, nad którą pracujemy.

R: Cel szczegółowy 3 krajowych ram zakłada zwiększenie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni. Jednym z ważniejszych sposobów jego realizacji jest zbudowanie mechanizmów współpracy pomiędzy sektorem prywatnym i publicznym. Jakie działania w tym zakresie podejmuje MC? Czy są plany przygotowywania specjalnego programu PPP w obszarze cyberbezpieczeństwa?

MAS: Za taki program można uznać np. program Cyberpark Enigma, który zakłada odtworzenie i rozbudowę krajowych kompetencji w obszarze budowy zdolności do kompleksowego wytwarzania urządzeń i oprogramowania. Będzie je można wykorzystywać we wszystkich gałęziach przemysłu. Zapewnieni to odpowiedni stopień cyberbezpieczeństwa. Ważnym elementem tego programu jest też projekt odtworzenia zdolności do produkcji mikroukładów, szczególnie na potrzeby szeroko rozumianego bezpieczeństwa narodowego oraz uzyskanie zdolności do certyfikacji takich wyrobów pod względem bezpieczeństwa.

W ramach realizacji tego celu przewidziane jest także przystąpienie strony rządowej do różnego rodzaju programów z zakresu bezpieczeństwa prowadzonych przez wiodących producentów sprzętu i oprogramowania.

R: Krajowe ramy stawiają sobie za zadanie zwiększenie bezpieczeństwa teleinformatycznego usług kluczowych i infrastruktury krytycznej. W polskim ustawodawstwie mamy już wypracowane pojęcie infrastruktury krytycznej oraz mechanizmy jej ochrony. Jaka będzie zależność pomiędzy operatorami wyznaczanymi przez RCB jako operatorzy infrastruktury krytycznej oraz operatorami zdefiniowanymi jako operatorzy usług kluczowych na mocy dyrektywy NIS?

MAS: Nie zawsze operatorzy usług kluczowych będą jednocześnie operatorami infrastruktury krytycznej. Niemniej taka zależność będzie często zachodzić. Pracując nad projektem ustawy o krajowym systemie cyberbezpieczeństwa MC ścisłe współpracuje z RCB. Chodzi o taką konstrukcję przepisów, by nie doszło do dublowania się obowiązków operatorów usług kluczowych, którzy jednocześnie są operatorami infrastruktury krytycznej.

Magdalena Wrzosek

Dyrektywa NIS – dostawcy usług cyfrowych i aneks III

Przyjęta 6 lipca 2016 dyrektywa NIS[2] wprowadza szereg regulacji i obejmuje dwa typy podmiotów. Operatorów usług kluczowych (OUK), a więc podmiotów zidentyfikowanych przez państwa członkowskie w sektorach wymienionych w Aneksie II Dyrektywy. Są to: sektor energetyki (energia elektryczna, ropa naftowa, gaz), transportowy (transport lotniczy, kolejowy, wodny i drogowy), bankowość, infrastruktura rynków finansowych oraz służba zdrowia, zaopatrzenie w wodę pitną i jej dystrybucja, a także infrastruktura cyfrowa. Drugi typ podmiotów objętych zakresem dyrektywy to dostawcy usług cyfrowych (DSP) wymienieni w aneksie III – **internetowe platformy handlowe, wyszukiwarki internetowe i usługi przetwarzania w chmurze.** Tym, co zwykle podkreśla się w analizach Dyrektywy NIS jest fakt, że dostawców usług cyfrowych obowiązuje odmienny reżim prawny, niż ten, którym objęci zostali operatorzy usług kluczowych.

[2] *Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii z 6 lipca 2016 r.*

Tzw. *light touch approach* oznacza przede wszystkim, że państwa członkowskie nie mogą wprowadzić regulacji silniejszych, niż te przewidziane w Dyrektywie.

Warto jednak zwrócić uwagę na jeszcze jeden istotny aspekt – współzależności, jakie występują pomiędzy operatorami usług kluczowych a dostawcami usług cyfrowych. Jest to aspekt często pomijany w analizach Dyrektywy NIS. Tymczasem, z dwóch powodów, wydaje się jednym z kluczowych. Po pierwsze, **objęcie dostawców usług cyfrowych lżejszą regulacją, sprawia, że zależni od nich operatorzy usług kluczowych powinni zidentyfikować procesy, zależne od tych usługodawców. Po drugie, zespół CSIRT właściwy dla dostawców usług cyfrowych nie będzie miał informacji o incydentach w takim zakresie, w jakim otrzymywać je będzie CSRT właściwy dla usług kluczowych.**

Dyrektywa wprowadza definicje dostawców usług cyfrowych. Zgodnie z nimi, **internetowa platforma handlowa** umożliwia konsumentom i przedsiębiorcom handlowym zawieranie umów sprzedaży lub umów o świadczenie usług online, równocześnie będąc ostatecznym miejscem zawierania tych umów. Oznacza to, że usługi online, które jedynie pośredniczą wobec stron trzecich lub też porównują ceny, nie są objęte regulacją. Dodatkowo usługi komputerowe świadczone przez internetową platformę handlową mogą obejmować przetwarzanie transakcji, agregowanie danych lub profilowanie użytkowników. W związku z tym internetowymi platformami handlowymi są sklepy z aplikacjami, które działają, jako sklepy internetowe umożliwiające cyfrową dystrybucje aplikacji lub oprogramowania stron trzecich.

Wyszukiwarka internetowa to „usługa cyfrowa, która umożliwia wyszukiwanie – co do zasady – wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania na jakikolwiek temat przez podanie słowa kluczowego, wyrażenia lub innej wartości; w wyniku przedstawia ona odnośniki, pod którymi można znaleźć informacje związane z zadanym pytaniem".[3] Zgodnie z tą definicją, Dyrektywa NIS nie obejmuje funkcji wyszukiwania, które ograniczają się do treści na konkretnej stronie internetowej (bez względu na to, czy funkcja wyszukiwania jest zapewniana przez wyszukiwarkę zewnętrzną). Zakresem Dyrektywy nie są także objęte usługi online, które porównują cenę produktów lub usług różnych przedsiębiorców, a następnie przekierowują użytkownika do preferowanego przedsiębiorcy, aby tam dokonał zakupu produktu.

„Usługa przetwarzania w chmurze oznacza usługę cyfrową umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania".[4] Przy czym pojęcie „skalowalne" odnosi się do zasobów komputerowych, które są elastycznie przydzielane przez dostawcę usługi niezależnie od położenia geograficznego zasobów, jako reakcja na fluktuację zapotrzebowania. Natomiast pojęcie „wspólne wykorzystywanie" jest używane do opisu zasobów obliczeniowych udostępnianych wielu użytkownikom, którzy dzielą wspólny dostęp do usługi. Przetwarzanie odbywa się przy tym oddzielnie dla każdego z użytkowników, mimo że usługa jest świadczona z tego samego sprzętu elektronicznego.

Zgodnie z artykułem 16 punkt 5 Dyrektywy NIS „w przypadku, gdy do celów świadczenia usługi, która ma istotne znaczenie dla utrzymania krytycznej działalności społecznej i gospodarczej, operator usług kluczowych jest zależny od dostawcy usług cyfrowych będącego stroną trzecią, operatorowi temu zgłasza się wszelki istotny wpływ na ciągłość usług kluczowych związany z incydentem, który dotyczy dostawcy usług cyfrowych". Aby jednak zgłoszenie takie było możliwe, w pierwszej kolejności konieczne jest właściwe zmapowanie procesów operatorów, usług kluczowych, zależnych od dostawców usług cyfrowych.

Warto przy tym zaznaczyć, że o ile w przypadku operatorów usług kluczowych istotny skutek zakłócający określany jest na podstawie sześciu kryteriów, o tyle w przypadku dostawców usług cyfrowych pod uwagę branych jest pięć czynników. W przypadku operatorów usług kluczowych są to: liczba **użytkowników zależnych od usługi świadczonej przez dany podmiot; zależność innych sektorów kluczowych, od usługi** świadczonej przez ten podmiot; **wpływ, jaki incydenty** – jeżeli chodzi o ich skalę i czas trwania – **mogłyby mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne, udział tego podmiotu w rynku, zasięg geograficzny** związany z obszarem, którego mógłby dotyczyć incydent **oraz znaczenie podmiotu w utrzymywaniu wystarczającego poziomu usługi przy uwzględnieniu dostępności alternatywnych sposobów świadczenia tej usługi.** Oprócz tych czynników międzysektorowych, państwa członkowskie mogą także uwzględniać czynniki sektorowe (np. wielkość lub udział w krajowej produkcji energii w odniesieniu do dostawców energii, dzienną wielkość dostaw w odniesieniu do dostawców ropy naftowej czy udział w wolumenie ruchu krajowego i roczną liczbę pasażerów lub przewozów towarowych w doniesieniu do transportu lotniczego, transportu kolejowego i portów morskich). Natomiast **w przypadku dostawców usług cyfrowych**, w celu określenia istotności incydentu bierze się pod uwagę: **liczbę użytkowników**, których dotyczy incydent, w szczególności użytkowników zależnych od usługi na potrzeby świadczenia ich własnych usług; **czas trwania incydentu; zasięg**

[3] *art 4.17 Dyrektywy 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.*

[4] *art 4.18 Dyrektywy 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.*

geograficzny, którego dotyczy incydent; **zasięg zakłócenia funkcjonowania usługi i zasięg wpływu na działalność gospodarczą i społeczną.**

Także inaczej, niż w przypadku operatorów usług kluczowych, dla dostawców usług cyfrowych to nie państwa członkowskie ustalać będą progi istotności incydentu. Powodem tego jest fakt, że są to dostawcy międzynarodowi (dostarczają usługi w wielu państwach członkowskich). Aby nie wprowadzać fragmentaryzacji rynku, a więc nie tworzyć sytuacji gdzie jeden podmiot będzie musiał się stosować do 28 reżimów prawnych, podjęto decyzję, że kwestia ta będzie uregulowana z poziomu europejskiego.[5] W związku z tym, w lutym 2018 roku, ENISA przygotowała rekomendacje na temat zgłaszania przez DSP incydentów w kontekście Dyrektywy NIS (*Incident notification for DSPs in the context of the NIS Directive. A comprehensive guideline on how to implement incident notification for Digital Service Providers, in the context of the NIS Directive*).[6]

W dokumencie tym, zaproponowano konkretne rozwiązania związane z określaniem istotności incydentów dostawców usług cyfrowych. W toku analiz wyznaczono cztery parametry, które powinny być brane pod uwagę: zasięg geograficzny (oznaczony jako P1), czas zakłócenia dostarczania usługi (oznaczony jako P2), liczba użytkowników dotkniętych incydentem oraz czas trwania incydentu (P3), wpływ na działalność społeczną i gospodarczą (P4).

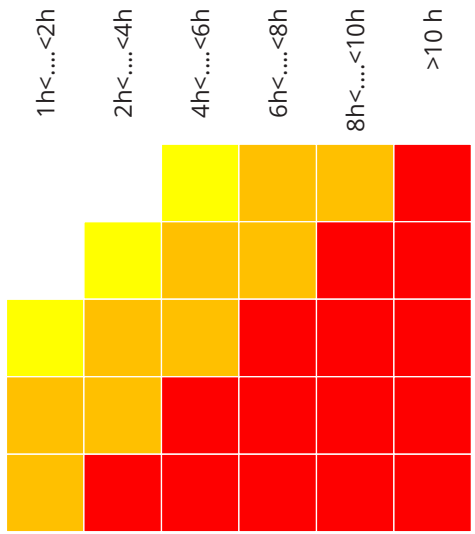
Dla trzech parametrów: P1, P2 i P4 zaproponowano trzystopniową skalę, gdzie:

1. poziom czerwony oznacza poważny incydent, wpływający na ciągłość usług dla wielu osób w kilku państwach członkowskich i powodujący bardzo duży wpływ gospodarczy i społeczny (jako czerwone muszą przy tym zostać oznaczone parametry P1, P2 i P4)
2. poziom pomarańczowy oznacza poważny incydent, dotykający wielu ludzi z jednego kraju i powodujący wysoki wpływ gospodarczy i społeczny (jako pomarańczowy musi przy tym zostać oznaczony jeden z parametrów – P1, P2 lub P4)
3. poziom żółty oznacza znaczący incydent, dotykający wiele osób w częściach kraju i powodujący skutki gospodarcze i społeczne (jako żółty musi przy tym zostać oznaczony jeden z parametrów – P1, P2 lub P4)

Natomiast w przypadku parametru P3 wyznaczono jednostkę „użytkownik/czas" (usertime), której za pomocą, którego DSP powinny określać czy zakłócenie spowodowane incydentem przekracza progi w ujęciu użytkownik – czas. Progi te obrazuje poniższa tabela.

Względny próg

(szacowana wielkość populacji kraju członkowskiego lub ilość klientów dostawcy usługi cyfrowej)



Dostawcy usług cyfrowych nie będą raportować w taki sposób, jak operatorzy usług kluczowych. Przede wszystkim obowiązek zgłaszania incydentu ma miejsce tylko wtedy, kiedy dostawca usług cyfrowych ma dostęp do informacji niezbędnych do oceny incydentu względem parametrów, o których mówi Dyrektywa. Dodatkowo taki incydent jest zgłaszany w państwie, gdzie dane DSP ma główną siedzibę. Oznacza to, że bez właściwego zdefiniowania współzależności pomiędzy DSP a OUK, państwa członkowskie mogą mieć problem z uzyskaniem wszystkich niezbędnych informacji w zakresie stanu cyberbezpieczeństwa, bo nie będzie wiadomo, do jakich innych państw należy zgłaszać się po potrzebne informacje. Jest to szczególnie kłopotliwe w przypadku małych państw, takich jak Estonia.

Ostatnią istotną kwestią w kontekście DSP jest problem z ich identyfikacją. Zgodnie z badaniem, przeprowadzonym przez ENISA, państwa członkowskie nie mają zidentyfikowanych tych typów dostawców. Dlatego najwłaściwszym sposobem ich identyfikacji może być właśnie wyjście od strony operatorów usług kluczowych i zmapowanie ich zależności od internetowych platform handlowych, wyszukiwarek internetowych i usług przetwarzania w chmurze.

[5] *Na mocy artykułu 8, Komisja Europejska ma przygotować akty wykonawcze, które doprecyzują paramenty dla istotnych skutków zakłócających w przypadku DSP.*

[6] *https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive/*

Mateusz Górnisiewicz

Bezpieczeństwo w sektorze finansowym: Dyrektywa PSD2 i nowe usługi płatnicze oparte o dostęp stron trzecich do rachunków

W listopadzie 2015 r. przyjęta została Druga Dyrektywa 2366 ws. usług płatniczych w ramach rynku wewnętrznego (tzw. Dyrektywa PSD2). Poprzez usankcjonowanie zupełnie nowego rodzaju usług płatniczych tj. usług opartych o dostęp do stron trzecich, wprowadza ona swoistą rewolucję na rynku UE. Działanie stron trzecich polega na tym, że klient – zamiast logować się bezpośrednio do swojej usługi bankowości elektronicznej – loguje się do zewnętrznego dostawcy usług płatniczych. Potem w imieniu klienta strona trzecia loguje się do dostawcy prowadzącego rachunek klienta (np. banku) i wykonuje operacje niezbędne do zrealizowania usługi, takiej jak np. zainicjowanie płatności czy pobranie i zagregowanie danych z rachunku bankowego w celu ułatwienia użytkownikowi zarządzania domowym budżetem. Poniższa tabela zawiera definicje nowego rodzaju usług płatniczych realizowanych przez stronę trzecią.

Usługa inicjacji płatności (ang. Payment Initiation Service)	Strona trzecia w imieniu klienta przekazuje zlecenie płatności na jego rachunku płatniczym – dzięki temu może np. od razu przekazać do odbiorcy płatności informację o tym, że płatność została zainicjowana
Usługa dostępu do informacji o rachunku (ang. Account Information Service)	Strona trzecia w imieniu klienta pobiera informacje o jego rachunku płatniczym (np. historię operacji czy bieżące saldo) – dzięki temu może np. ułatwić klientowi zarządzanie budżetem domowym, czy też zweryfikować informacje potrzebne do obliczenia jego zdolności kredytowej
Usługa potwierdzenia dostępności środków na rachunku (ang. Confirmation of Availabiliy of Funds Service)	Strona trzecia w imieniu klienta sprawdza, czy na jego rachunku płatniczym znajdują się środki wystarczające na zrealizowanie określonej transakcji

Tego typu usługi były już dostępne na rynku Unii Europejskiej (również w Polsce), jednak dotychczas korzystanie z nich – w przypadku, gdy klient udostępniał stronie trzeciej dane uwierzytelniające do swojego rachunku płatniczego – powodowało łamanie przez klientów reguły ustanowionej w art. 56(2) poprzedniej Dyrektywy ws. Usług Płatniczych: „użytkownik usług płatniczych podejmuje w szczególności, z chwilą otrzymania instrumentu płatniczego, wszelkie stosowne kroki w celu zapobieżenia naruszeniu indywidualnych zabezpieczeń tego instrumentu".

Obecnie Dyrektywa wprowadza dla dostawców usług płatniczych (w tym banków) obowiązek umożliwienia stronom trzecim świadczenia takich usług, bez konieczności zawierania relacji umownej pomiędzy stroną trzecią a dostawcą prowadzącym rachunek. Szczegółowe wymagania techniczne dotyczące sposobu funkcjonowania tych usług opisane zostaną w dokumencie „Regulacyjne Standardy Techniczne (ang. Regulatory Technical Standard – RTS), którego przyjęcie przewidywane jest w listopadzie 2017 r., a którego projekt został opublikowany przez Europejski Urząd Nadzoru Bankowego (EBA). Zgodnie z tym projektem, dopuszczalne jest podejście polegające na udostępnianiu przez klientów stronom trzecim danych uwierzytelniających do ich rachunków płatniczych tak, aby strony trzecie „przepisując" te dane mogły logować się w imieniu klientów do ich bankowości elektronicznej. Tego rodzaju usługi są już dostępne w Unii Europejskiej i zazwyczaj opierają się o technikę tzw. screen scraping, czyli polegają na zbudowaniu interfejsu z systemem bankowości elektronicznej w sposób umożliwiający „emulowane klikanie" przez aplikację strony trzeciej w serwisie internetowym bankowości elektronicznej klienta. Poniższy schemat przestawia sposób działania strony trzeciej.

O ile fakt umożliwienia świadczenia tych usług w ramach regulacji prawnych jest pozytywny (choćby w świetle rozwoju innowacyjnych usług), to warto zwrócić uwagę na szereg zagrożeń, które może generować nieodpowiedzialne podejście do implementacji tych zapisów. W takim przypadku można mówić o kilku zagrożeniach :

- Nie występowałaby w praktyce techniczna możliwość skutecznego zabezpieczenia przed sytuacją, w której np. osoba mająca dostęp do infrastruktury teleinformatycznej strony trzeciej lub twórca wykorzystywanego przez nią oprogramowania wszedłby w posiadanie danych uwierzytelniających klienta i wykorzystał je w celu popełnienia nadużycia - potencjalnie na szeroką skalę, co powodowałoby istotne ryzyko systemowe dla sektora usług płatniczych,

- Nastąpiłoby drastyczne ograniczenie skuteczności podstawowej zasady bezpieczeństwa wpajanej od wielu lat klientom m.in. w Polsce (zarówno przez dostawców usług płatniczych, jak i organy nadzoru), mówiącej o tym, że należy dbać o poufność swoich danych logowania do bankowości elektronicznej i – w szczególności – nikomu ich nie udostępniać; należy tu zwrócić uwagę, że to właśnie użytkownik końcowy jest zazwyczaj najsłabszym ogniwem łańcucha zabezpieczeń,

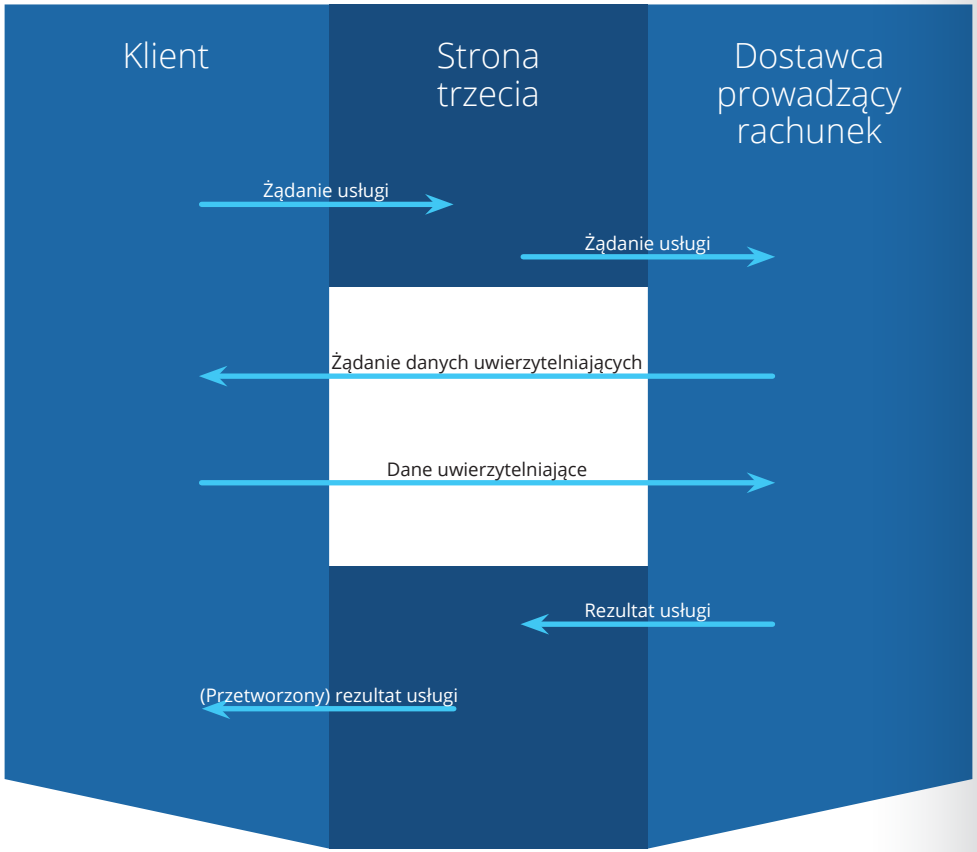
- Cyberprzestępcy przeprowadzający ataki phishingowe uzyskaliby znaczące ułatwienie dzięki nowemu wektorowi ataku, tj. możliwości podszywania się pod licencjonowane strony trzecie w celu wyłudzenia danych uwierzytelniających klientów bankowości elektronicznej,

- Ponieważ dostawca prowadzący rachunek komunikowałby się jedynie ze stroną trzecią, nie miałby on dostępu do danych specyficznych dla urządzenia danego klienta, które to dane są w istotnym stopniu wykorzystywane w ramach funkcjonowania systemów bankowych zabezpieczających klientów i ich środki finansowe przed nadużyciami,Strona trzecia miałaby utrudnioną możliwość przekazania dostawcy prowadzącemu rachunek (bankowi) informacji o swojej własnej tożsamości oraz o tym, że komunikuje się on właśnie ze stroną trzecią, a nie bezpośrednio z klientem, a zatem dostawca prowadzący rachunek nie mógłby zablokować dostępu do wrażliwych danych płatniczych klienta (co również jest wymagane w projekcie RTS).

Na koniec należy zauważyć, że podnoszony niekiedy (np. na forum unijnym podczas dyskusji nad projektem RTS) argument mówiący o konieczności zapewnienia zasad uczciwej konkurencji dla istniejących stron trzecich, które

od kilku lat świadczą usługi wchodząc w posiadanie danych uwierzytelniających do bankowości elektronicznej (czyli zgodnie z omówionym powyżej podejściem), wydaje się być nie w pełni zasadny, biorąc pod uwagę fakt, że korzystanie z takich usług w świetle poprzedniej Dyrektywy powodowało łamanie przez klientów ustanowionej w jej art. 56(2) reguły dotyczącej konieczności zabezpieczenia danych uwierzytelniających.

Rozwiązaniem powyższych problemów – przy jednoczesnym zapewnieniu realizacji jednego z celów PSD2, czyli wsparcia rozwoju nowoczesnych usług płatniczych – jest przyjęcie podejścia, w którym po uruchomieniu przez klienta danej usługi strony trzeciej, będzie on przekierowywany do swojego dostawcy prowadzącego rachunek (np. na jego stronę internetową lub do aplikacji) w celu uwierzytelnienia, a następnie dostawca ten przekaże stronie trzeciej odpowiedni zakres danych wymaganych do realizacji danej usługi. Proces ten przedstawiony został na poniższym schemacie.



Zaproponowane rozwiązanie jest o wiele bezpieczniejsze od podejścia omówionego wcześniej, a jednocześnie gwarantuje możliwość rozwoju rynku innowacyjnych usług płatniczych. Po pierwsze: poprzez ograniczenie niechęci części klientów do przekazywania ich poufnych danych logowania nieznanym im bliżej podmiotom (stronom trzecim), znacząco zwiększyłaby się możliwość wejścia na ten rynek nowych, innowacyjnych firm i usług płatniczych. Po drugie: w warstwie technicznej, w przypadku stosowania przez banki zaawansowanych metod uwierzytelniania klientów (np. biometrii), podejście takie znosi barierę technologiczną związaną z koniecznością odwzorowywania takich metod przez strony trzecie.

Jednocześnie w sytuacji, w której techniczne aspekty komunikacji pomiędzy dostawcami prowadzącymi rachunki a stronami trzecimi realizowane będą zgodnie z powszechnie obowiązującym standardem jednolitego API (ang. Application Programming Interface), koszt rozpoczęcia świadczenia takich usług przez strony trzecie będzie znacząco ograniczony, co dodatkowo przyczyni się do rozwoju innowacyjności.

Taki standard opracowywany jest obecnie przez Związek Banków Polskich (z udziałem zarówno banków, jak i innych dostawców usług płatniczych). Podstawowym założeniem standardu jest zapewnienie jak największego bezpieczeństwa użytkownikom usług płatniczych, w tym przede wszystkim taka jego konstrukcja, aby strony trzecie na żadnym etapie nie wchodziły w posiadanie danych uwierzytelniających klientów. W inicjatywę włączonych jest obecnie ponad 100 osób reprezentujących instytucje współpracujące ze Związkiem Banków Polskich i znajduje się ona na zaawansowanym etapie. Przygotowany projekt zakłada oparcie się o standard autoryzacji OAuth 2.0, usługi sieciowe typu RESTful oraz JSON jako format wymiany danych. Ukończenie specyfikacji technicznej interfejsu możliwe będzie po zweryfikowaniu jej zgodności z ostatecznym dokumentem RTS - po jego spodziewanej publikacji w listopadzie 2017 r.

Pozostaje mieć nadzieję, że finalna wersja regulacji pozwoli na utrzymanie podejścia, w którym nie będzie wymagane umożliwienie świadczenia opisanych tu usług w oparciu o przekazywanie stronom trzecim danych logowania – w innym przypadku całkiem realny stanie się scenariusz pojawienia się firmy płatniczej typu „Amber Pay" o skali działalności obejmującej całą Unię Europejską.

Flash z Komisji Europejskiej

Katarzyna Ananicz, Anna Podgórska – Buompane, Justyna Romanowska

Stałe Przedstawicielstwo przy Unii Europejskiej w Brukseli

W styczniu 2017 roku w Stałym Przedstawicielstwie przy Unii Europejskiej w Brukseli, Ministerstwo Cyfryzacji utworzyło trzyosobowy zespół do spraw cyfrowych (wcześniej tymi kwestiami zajmowała się jedna osoba). Natomiast w marcu 2017 r. Premier Beata Szydło powołała Pełnomocnika ds. Jednolitego Rynku Cyfrowego. Funkcję tą sprawuje Minister Krzysztof Szubert – Sekretarz w Ministerstwie Cyfryzacji.

W ramach współpracy Stałego Przedstawicielstwa i NASK powstaje rubryka w której regularnie publikowane będą informacje na temat działań podejmowanych w zakresie różnych inicjatyw związanych z Jednolitym Rynkiem Cyfrowym.

Od czerwca prezydencje w Radzie Unii Europejskiej sprawuje Estonia, która priorytetowo traktuje kwestie cyberbezpieczeństwa. **We wrześniu ma się ukazać komunikat KE – propozycja rewizji strategii Cyberbezpieczeństwa UE oraz nowego mandatu dla Europejskiej Agencji Bezpieczeństwa Sieci i Informacji.** Ponad to mają być przedstawione nowe propozycje dotyczące ram certyfikacji.

Komentarz NASK:

Strategia bezpieczeństwa cybernetycznego UE: otwarta i bezpieczna i chroniona cyberprzestrzeń[7] to pierwszy strategiczny dokument UE w tematyce cyberbezpieczeństwa. Została **przyjęta w 2013** i razem z nią KE przedstawiła projekt tzw. dyrektywy NIS. W związku z przyjęciem dyrektywy w lipcu 2016 pojawiła się konieczność rewizji dokumentu.

Europejska Agencja Bezpieczeństwa Sieci i Informacji to unijna agencja, stanowiąca ośrodek specjalistycznej wiedzy w zakresie bezpieczeństwa cybernetycznego w Europie, który pomaga Unii Europejskiej i należącym do niej krajom zapobiegać problemom dotyczącym bezpieczeństwa ICT. Agencja została **powołana w 2004** (Regulacja EC no 460/2004). ENISA otrzymała wtedy mandat na 5 lat, ale był on przedłużany dwukrotnie w 2009 i 2011 roku. W 2013 roku Parlament Europejski przyjął nową regulacje 526/2013, która zastąpiła tą z 2004 roku, która stanowi obecnie prawne podstawy działania Agencji. W Komunikacie do Parlamentu Europejskiego w sprawie wzmacniania europejskiego systemu odporności cybernetycznej oraz wspierania konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego[8], Komisja Europejska zapowiedziała, **że do końca 2017 roku zakończy ocenę ENISY, uwzględniając potrzebę modyfikacji lub rozszerzenia mandatu** Agencji, tak aby jak najszybciej przedstawić wniosek w sprawie nowego mandatu.

W czerwcu br. KE przedstawiła ocenę skutków regulacji w tej sprawie. Obecnie rozpatrywane są dwie możliwości. Pierwsza z nich to odnowienie mandatu

[7] *http://www.europarl.europa.eu/meetdocs/2009_2014/documents/join/com_join(2013)0001_/com_join(2013)0001_pl.pdf*

[8] *http://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A52016DC0410*

ENISY jako agencji będący ośrodkiem doradczym, wspierającym państwa członkowskie w implementacji polityk z zakresu cyberbezpieczeństwa, oraz certyfikacji produktów ICT, a także organizującej ćwiczenia, inicjującej współpracę pomiędzy państwami członkowskimi (zwłaszcza w obliczu incydentów międzynarodowych). Drugi wariant zakłada wyposażenie Agencji nie tylko w wymienione w poprzednim wariancie kompetencje z zakresu policy, ale także w pełne zdolności operacyjne, a więc wsparcie państw członkowskich w zakresie zapobiegania, wykrywania i reagowania na incydenty teleinformatyczne.

Negocjowane są zapisy Kodeksu Łączności Elektronicznej. Główną osią sporu z Komisją Europejską i Parlamentem Europejskim będzie kwestia zarządzania widmem radiowym i próba wprowadzenia większej harmonizacji oraz centralizacji na poziomie UE. Zmiany obejmują również kwestie dostępu telekomunikacyjnego oraz inwestycji w nowoczesne sieci telekomunikacyjne. Zmieniana jest również definicja usług łączności elektronicznej, w które wg propozycji KE mają wejść również tzw. OTTs czy usługi M2M. Ponadto, zmieniane są zasady dot. zakresu i finansowania usługi powszechnej. UE idzie w kierunku zastąpienia dostępu stacjonarnego (głos) dostępem do internetu szerokopasmowego. To tylko niektóre z proponowanych przez KE zmian. W MC odbywają się regularne spotkania konsultacyjne w tej sprawie, na które zapraszane są zainteresowane podmioty.

Prowadzone są negocjacje rozporządzenia o e-prywatności: propozycja Komisji budzi wiele wątpliwości państw członkowskich – m.in. dot. zgodności z rozporządzeniem o ochronie danych osobowych, kwestii zakresu (objęcie firm czy usług dodatkowych), retencji danych, organu odpowiedzialnego za nadzór, e-marketingu, działania tzw. „ciasteczek". Prezydencja Estonii przygotuje nowy tekst we wrześniu br.

Jesienią oczekiwana jest również propozycja legislacyjna dotycząca swobodnego przepływu danych w UE. Polska aktywnie zabiegała i zabiega o projekt, który w jasny sposób zabroni lokalizacji danych (przy zachowaniu pewnych wyjątków, m.in. dotyczących bezpieczeństwa). Dodatkowo Komisja przedstawi wytyczne dla platform w zakresie zdejmowania treści online (procedura „notice and take down").

Niedawno Rada UE wraz z PE uzgodniły projekt rozporządzenia WiFi4EU oraz 15 czerwca weszły w życie zmiany umożliwiające Roam Like at Home.

Dodatkowo, Stałe Przedstawicielstwo wspólnie z Ministerstwem Cyfryzacji, zainicjowało list 17 premierów UE do przewodniczącego Rady Europejskiej Donalda Tuska, wskazujący na potrzebę silniejszego wyeksponowania szeroko rozumianych kwestii cyfrowych na najwyższym poziomie politycznym UE[9].

[9] *https://mc.gov.pl/aktualnosci/polska-inicjatorem-listu-17-premierow-ue*

CYBERPOLICY

NASK

cyberpolicy.nask.pl