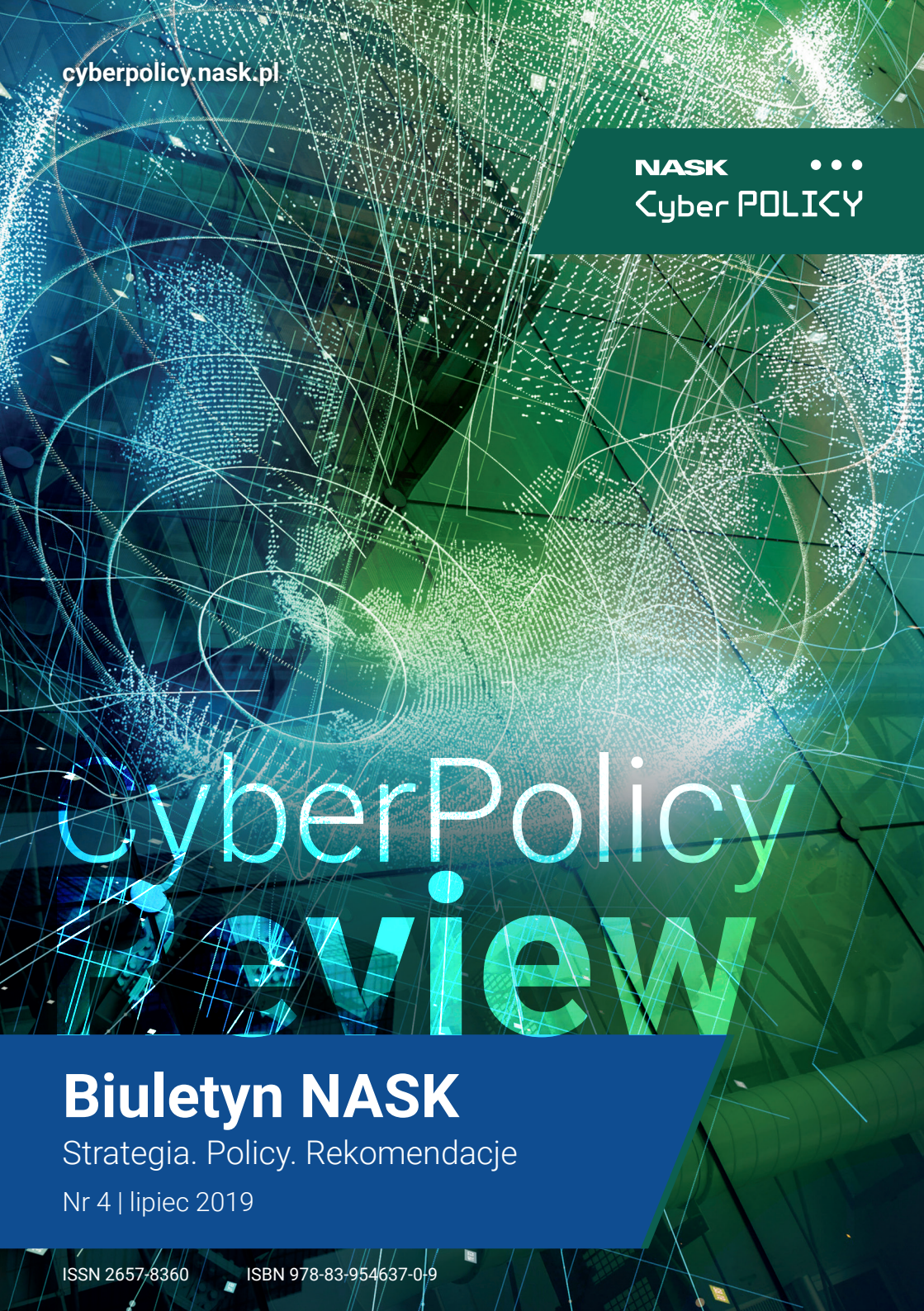


Biuletyn NASK

Strategia. Policy. Rekomendacje

Nr 4 | lipiec 2019

ISSN 2657-8360 ISBN 978-83-954637-0-9

NASK Cyber POLICY

Biuletyn NASK

Strategia. Policy. Rekomendacje.

Nr 4/lipiec 2019

Redakcja: Magdalena Wrzosek

ISSN 2657-8360

ISBN 978-83-954637-0-9

NASK PIB, Warszawa, 2019

Słowo wstępu

To już czwarty numer Biuletynu *CyberPolicy Review*. Miło mi poinformować, że doczekał się on numeru ISSN oraz ISBN. Jest to kolejny etap rozwoju działalności Państwowego Instytutu Badawczego NASK w zakresie prawnych i strategicznych aspektów cyberbezpieczeństwa i nowoczesnych technologii. W tym numerze pochylamy się nad reformą prawa telekomunikacyjnego w UE, certyfikacją ICT oraz działalnością badawczo – rozwojową.

Pod koniec 2018 roku został przyjęty Europejski Kodeks Łączności Elektronicznej. Jest to kompleksowa reforma regulacji telekomunikacyjnych (z 2009 roku) i jeden z istotniejszych projektów w zakresie Jednolitego Rynku Cyfrowego. Zmiany dotyczą dostępu do infrastruktury, regulacji widma radiowego oraz definicji i regulacji usług łączności elektronicznej. W tym numerze *CyberPolicy Review* przedstawiamy artykuł na temat ewolucyjnego podejścia zawartego w Kodeksie.

Od 27 czerwca br. obowiązuje natomiast Akt o Cyberbezpieczeństwie, który wprowadza certyfikacje ICT na poziomie europejskim. Temat ten podejmowaliśmy już w ostatnim numerze. Tym razem mamy przyjemność przedstawić artykuł, o polskim kontekście certyfikacji i związanymi z nią wyzwaniami.

Na koniec projekt SISSDEN, czyli badawczo – rozwojowa odpowiedź na potrzebę budowania świadomości w zakresie cyberbezpieczeństwa.

Zapraszam do lektury.

Krzysztof Silicki
Zastępca Dyrektora NASK PIB
– Dyrektor ds. Cyberbezpieczeństwa i Innowacji

Spis treści

Ignacy Święcicki

Europejski Kodeks Łączności Elektronicznej – ewolucja zamiast rewolucji

Ignacy Święcicki – Kierownik zespołu gospodarki cyfrowej w Polskim Instytucie Ekonomicznym. Poprzednio pracował w Ministerstwie Cyfryzacji, gdzie zajmował się europejskimi regulacjami w obszarze telekomunikacji, w tym odpowiadał za negocjacje Europejskiego Kodeksu Łączności Elektronicznej oraz ostatnich regulacji roamingowych. Brał również udział w opracowywaniu ocen skutków regulacji do nowych aktów prawnych i wytycznych do przeprowadzania oceny wpływu w rządowym procesie legislacyjnym. Doświadczenie analityczne zdobywał w think tanku demosEUROPA – Centrum Strategii Europejskiej. Absolwent ekonomii na Uniwersytecie Warszawskim.

Na Europejski Kodeks Łączności Elektronicznej można patrzeć z dwóch perspektyw. Z jednej strony dyrektywa jest **elementem strategii jednolitego rynku cyfrowego**. Wpisuje się w szereg inicjatyw mających pobudzić rozwój europejskiej gospodarki cyfrowej i zapewnić dotrzymanie kroku USA i Chinom – światowym liderom w tym obszarze.

Z drugiej, jest to **element ewolucji rynku telekomunikacyjnego w Europie** i jego regulacji. W tym sensie jest nowelizacją sektorowej regulacji, która wpisuje się w cykliczne prace prowadzone na poziomie UE oraz poszczególnych państw członkowskich. Napięcie między tymi perspektywami widać było zarówno w trakcie prac nad poszczególnymi artykułami, jak i w końcowym tekście.

Nowe epoka w świecie telekomunikacji

Kodeks poprzedziły regulacje telekomunikacyjne z 2001 roku, zaktualizowane w 2009 r. Było to pięć dyrektyw[1] i rozporządzenie o BEREC[2]. Jednak, w świecie technologii i telekomunikacji ostatnie dziesięć lat to cała epoka, a warunki rynkowe zmieniły się diametralnie.

- W **warstwie infrastrukturalnej** kluczowe znaczenie uzyskały sieci ruchome oraz, co za tym idzie, regulacje w obszarze widma radiowego. **Jedną z narracji towarzyszących pracom nad Kodeksem była konieczność wdrożenia w Europie sieci 5G**, wymagających zarówno nowych zasobów widma radiowego, jak i innego podejścia do lokalizowania stacji bazowych i nadajników. W warstwie kablowej technologie miedziane i kablowe przeszły kilka etapów rozwoju, a **coraz powszechniej zaczęły być stosowane sieci światłowodowe**, oferujące najwyższe parametry transmisji.
- W **warstwie usług** coraz większe znaczenie mają tak zwane usługi over-the-top (OTT), świadczone za pośrednictwem internetu, ale nie związane bezpośrednio z samą usługą dostępu do sieci. Spowodowało to również rozdzielenie podmiotów odpowiedzialnych za infrastrukturę od tych, które z niej korzystają – usługi OTT najczęściej świad-

[1] *Dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa) (Dz.U. L 108 z 24.4.2002, s. 33).*

Dyrektywa 2002/19/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie dostępu do sieci łączności elektronicznej i urządzeń towarzyszących oraz wzajemnych połączeń (dyrektywa o dostępie) (Dz.U. L 108 z 24.4.2002, s. 7).

Dyrektywa 2002/20/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie zezwoleń na udostępnienie sieci i usług łączności elektronicznej (dyrektywa o zezwoleniach) (Dz.U. L 108 z 24.4.2002, s. 21).

Dyrektywa 2002/22/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników (dyrektywa o usłudze powszechnej) (Dz.U. L 108 z 24.4.2002, s. 51).

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37).

[2] *BEREC to Organ Europejskich Regulatorów Łączności Elektronicznej – organizacja zrzeszająca krajowych regulatorów rynków łączności elektronicznej z krajów unijnych, jej misją jest koordynacja prac regulacyjnych i wspieranie Komisji Europejskiej np. przez zbieranie informacji, wydawanie opinii i raportów. Powołany Rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 1211/2009 z dnia 25 listopada 2009 r. ustanawiające Organ Europejskich Regulatorów Łączności Elektronicznej (BEREC) oraz Urząd (Dz.U. L. 337 z 18.12.2009, s. 1).*

czone są przez inne firmy niż operatorzy infrastruktury.

- W **warstwie komunikacji** na znaczeniu traciły SMSy i tradycyjna telefonia, a komunikacja przenosiła się do komunikatorów jak WhatsApp czy Messenger.

Dwa ostatnie czynniki skutkowały dynamicznie rosnącym wolumenem przesyłanych danych wymuszającym na operatorach inwestycje w pojemność sieci oraz spadkiem przychodów z dotychczasowych usług. Co istotne, **firmy działające w modelu OTT oraz komunikatory internetowe nie były objęte regulacjami typowymi dla sektora telekomunikacji**. Firmy telekomunikacyjne wskazywały, że z jednej strony są niejako zmuszone do inwestycji, a z drugiej konkurenci, których działalność jest w mniejszym stopniu regulowana, odbierają im użytkowników. Często spotykanym postulatem było więc wprowadzenie tzw. *level playing field,* czyli równych warunków konkurencji dla wszystkich podmiotów.

Nowa propozycja kodeksu – pięć obszarów regulacji

Sam Kodeks był tworzony po częściowo nieudanej propozycji jednolitego rynku telekomunikacyjnego (*telecommunications single market*, TSM), przedstawionej w 2013 roku przez poprzednią Komisję Europejską[3]. Tamten projekt, również zawierający szereg daleko idących zmian w obszarze dostępu do sieci czy widma radiowego, został bardzo negatywnie odebrany przez państwa członkowskie. Przyjęty na koniec dokument obejmował jedynie dwa obszary – neutralność sieci i roaming międzynarodowy[4]. Bazując na tych doświadczeniach Komisja przeprowadziła szeroko zakrojony proces konsultacji na etapie projektowania nowej propozycji.

Przedstawiony na jesieni 2016 projekt dyrektywy obejmował pięć obszarów regulacji:

1. strukturę instytucjonalną,
2. dostęp do sieci,
3. widmo radiowe,
4. usługę powszechną,
5. prawa użytkownika końcowego.

Ze względu między innymi na kończące się prace nad ogólnym rozporządzeniem o ochronie danych osobowych (RODO), Kodeks nie uwzględniał przeglądu dyrektywy ePrivacy. Zmiany w tym zakresie zostały przesunięte do odrębnego rozporządzenia[5].

[3] *Wniosek Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające środki dotyczące europejskiego jednolitego rynku łączności elektronicznej i mające na celu zapewnienie łączności na całym kontynencie, zmieniające dyrektywy 2002/20/WE, 2002/21/WE i 2002/22/WE oraz rozporządzenia (WE) nr 1211/2009 i (UE) nr 531/2012 (COM(2013) 627 final)*

[4] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/2120z dnia 25 listopada 2015 r. ustanawiające środki dotyczące dostępu do otwartego internetu oraz zmieniające dyrektywę2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, a także rozporządzenie (UE) nr 531/2012 w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii*

[5] *Wniosek ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej) (COM(2017) 10 final)*

[6] *Dyrektywa Parlamentu Europejskiego I RADY (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona) – Dalej „Kodeks"*

Ostatecznie przyjęty dokument nie różni się istotnie strukturą ani zakresem obszarów regulacyjnych od wyjściowej propozycji[6].

Cele Kodeksu

Przed omówieniem poszczególnych obszarów nowej dyrektywy warto przyjrzeć się ogólnym celom całej regulacji. Cele nie mają ustalonej hierarchii, a obejmują[7]:

- promowanie łączności, dostępu do sieci o bardzo dużej przepustowości oraz korzystania z tych sieci;
- promowanie konkurencji przy dostarczaniu sieci (w tym konkurencji opartej na infrastrukturze) oraz konkurencji przy świadczeniu usług;
- rozwój rynku wewnętrznego przez usuwanie przeszkód dla inwestycji i ujednolicanie pomiędzy poszczególnymi krajami warunków regulacyjnych, inwestycyjnych, w zakresie wykorzystania widma radiowego, świadczenia usług i innych elementów;
- wspieranie obywateli przez zapewnianie łączności, dostępności i korzystania z sieci o bardzo wysokiej przepustowości, w tym skutecznej konkurencji w zakresie możliwości wyboru, ceny i jakości usług, a także poprzez dbanie o bezpieczeństwo i ochronę użytkowników.

W stosunku do poprzednio obowiązującego zestawu celów widać znacznie większy nacisk na dostępność i korzystanie z sieci, a także na ujednolicanie warunków pomiędzy państwami członkowskimi. W pewnym zakresie nastąpiło również odejście od zasady neutralności technologicznej. Sieci o bardzo dużej przepustowości, do której odniesienie znajduje się zarówno w celach Kodeksu jak i w wielu szczegółowych regulacjach jest definiowana jako sieć światłowodowa lub inna – ale taka, która zapewnia podobną wydajność do sieci światłowodowej[8].

Struktura instytucjonalna

Kodeks na nowo reguluje podział obowiązków i zaangażowanie poszczególnych instytucji zaangażowanych w poszczególnych segmentach rynku telekomunikacyjnego. Przede wszystkim jasno podkreślona jest niezależność krajowych organów regulacyjnych (dalej: NRA) oraz wprowadzono minimalny katalog ich obowiązków. Celem było ujednolicenie struktur w krajach UE, a także ułatwienie współpracy regulatorów w ramach BEREC.

NRA, czyli krajowe organy regulacyjne

NRA odpowiadają jako wyłączne organy co najmniej za regulację rynku, w tym nakładanie obowiązków regulacyjnych, rozstrzyganie sporów między przedsiębiorstwami,

[7] *Art. 3*

[8] *Art. 2(2) Kodeksu*

ocenę i obliczanie kosztu netto świadczenia usługi powszechnej, przenoszenie numerów. Oprócz tego prowadzą sprawy związane z zarządzaniem widmem radiowym, choć państwa członkowskie mogą te zadania przydzielić innym organom. W takim przypadku NRA zapewnia tym organom doradztwo w zakresie kształtowania rynku i konkurencji na nim. Z kolei w obszarze ochrony praw użytkowników NRA mają się przyczyniać do tejże ochrony, w porozumieniu z innymi właściwymi organami[9].

Dyskusje nad katalogiem wyłącznych obowiązków NRA trwały niemal do końca negocjacji i angażowały wiele krajów. Określenie szerokiego katalogu obowiązków zastrzeżonego dla konkretnej instytucji wymusiłoby zmiany w wielu krajach członkowskich – przykładowo we Francji czy Holandii instytucja odpowiadająca za widmo radiowe jest odrębna od regulatora. Takie rozwiązanie oznaczałoby też pozbawienie rządów części wpływu, gdyż Kodeks przewiduje silną niezależność organu regulacyjnego. Z tych powodów z katalogu usunięto proponowane na początku przez Komisję Europejską wyłączne kompetencje w zakresie widma radiowego, udzielanie zezwoleń ogólnych (czyli dopuszczenia podmiotu do funkcjonowania na rynku) czy zarządzanie zasobami numeracyjnymi.

Niezależność NRA przejawia się m.in. określeniem sposobu powoływania szefa organu (przejrzysty i otwarty konkurs), brakiem możliwości odwołania w trakcie kadencji poza przypadkiem złamania warunków wymaganych w momencie powołania, a także koniecznością zapewnienia odpowiednich zasobów technicznych, finansowych i ludzkich. NRA nie mogą też przyjmować żadnych instrukcji od innych podmiotów – co oznacza brak możliwości bezpośredniego wpływania decydentów politycznych na sfery regulacji zarezerwowane wyłącznie dla krajowego organu regulacyjnego[10].

Pozostała struktura instytucjonalna

Poza organami krajowymi struktura instytucjonalna składa się w głównej mierze z:

- BEREC (*Body of European Regulators for Electronic Communications*) – Organ Europejskich Regulatorów Łączności Elektronicznej – organizacja zrzeszająca krajowych regulatorów rynków łączności elektronicznej z krajów unijnych.
- RSPG (*Radio Spectrum Policy Group*) – zespół ds. polityki widma radiowego, w którego pracach udział biorą przedstawiciele rządów i NRA.
- Komisja Europejska.

To w gronie tych instytucji decydować się będą szczegóły nowych regulacji i ich praktycznego stosowania. **BEREC** w wielu obszarach wypracowuje wytyczne dla stosowania poszczególnych przepisów Kodeksu[11], a w innych wydaje opinie, które Komisja musi uwzględniać w swoich decyzjach.

RSGP z grupy służącej Komisji radą w sprawach widma radiowego, zmienia się w kluczowy organ koordynujący ten aspekt polityki, w tym odpowiadającym za organizację procedury wzajemnej oceny postępowań dotyczących przydziału widma radiowego (o czym szerzej w dalszej części tekstu).[12]

Komisja Europejska wyda szereg aktów implementacyjnych do Kodeksu, a wspierać ją w tym będzie Komitet ds. widma radiowego (RSC). W tym kontekście warto podkreślić, że w porównaniu do obecnego stanu, znaczącemu wzmocnieniu uległa rola RSPG i BEREC, natomiast niewielkie zmiany zaszły w możliwościach kontrolnych Komisji Europejskiej. W wyjściowej propozycji Komisja zastrzegła dla siebie szersze prerogatywy (np. możliwość wetowania decyzji regulacyjnych, wydawania z własnej inicjatywy decyzji w sprawach transgranicznych porozumień co do widma radiowego), jednak te propozycje nie zostały przyjęte przez państwa członkowskie.

Widmo radiowe

Widmo radiowe było przedmiotem szczególnie napiętych dyskusji. Komisja Europejska chciała wzmocnienia centralnego nadzoru nad przydzielaniem zasobów widma radiowego w Europie. Wprawdzie propozycja nie zawierała koncepcji wspólnego regulatora, jednak proponowano obowiązkowy mechanizm wzajemnej oceny postępowań dotyczących przydziału widma radiowego. Komisja dążyła do zagwarantowania sobie możliwo-

[9] *Art. 5*

[10] *Art. 5-9*

[11] *Np. Art. 12 – wzór zgłoszeń przy zezwoleniu ogólnym, 22 – analizy geograficzne, 61 – lokalizacja zakończenia sieci, 69 – minimalne kryteria dotyczące oferty ramowej*

[12] *Por. m.in. Art. 4 i art. 35*

ści kontroli krajowych postępowań, co było argumentowane z jednej strony przykładami źle skonstruowanych przepisów, a z drugiej koniecznością harmonizacji polityki widma radiowego w UE. Harmonizacja miała zwiększyć skalę rynku europejskiego, ułatwić działanie firmom i umożliwić im szybszy rozwój. Końcowe zapisy utrzymały mechanizm konsultacji i wzajemnej oceny, jednak jest on dobrowolny i prowadzony przez RSPG[13].

5G – długość praw do widma radiowego

Jednocześnie przyszły rozwój sieci 5G był argumentem dla innych zmian w obszarze widma radiowego. Przede wszystkim w Kodeksie wskazano, że w przypadku wydania wyłącznych praw do widma radiowego, takie rezerwacje muszą obowiązywać przez przynajmniej 15 lat, a na kolejne 5 będą przedłużane niemal automatycznie[14]. **To istotna zmiana, ponieważ w myśl obecnych przepisów, decydujący głos odnośnie do długości rezerwacji mają organy krajowe**. Polskie przepisy wprost określają, że maksymalna długość okresu, na jaki przyznawane są prawa to 15 lat[15]. Operatorzy telekomunikacyjni, jako argument za wydłużeniem okresu, na który przyznawane są prawa do widma, podnosili kwestie przewidywanych kosztów inwestycji. W związku ze specyfiką sieci 5G (m.in. wiele małych komórek) koszty jej budowy mogą być bardzo wysokie, a dłuższy okres wyłącznych praw do widma zachęcałby firmy do inwestycji. Na potrzeby sieci 5G w Kodeksie wskazano też konkretną datę, 31 grudnia 2020 r., do której pasma 3,4-3,8 GHz i 26 GHz mają zostać udostępnione na potrzeby bezprzewodowej, szerokopasmowej łączności[16].

Z punktu widzenia Polski w obszarze widma radiowego kluczowe było uwzględnienie specyficznej sytuacji naszego kraju. Jako że Polska ma trzech sąsiadów spoza UE, negocjacje związane z wykorzystaniem widma radiowego są bardziej złożone. W Kodeksie zawarto odpowiednie zapisy, obligujące Unię Europejską do wspierania poszczególnych państw członkowskich w negocjacjach z krajami trzecimi[17], a także przewidziano odpowiednią przesłankę w przypadku derogacji (tzn. uchylenia części normy prawnej) od decyzji harmonizacyjnych. Kraje z niezakończoną koordynacją z sąsiadami spoza UE mogą opóźnić wdrożenie decyzji harmonizacyjnych i nie poniosą za to konsekwencji[18].

5G – ułatwienie wdrażania punktów dostępu bezprzewodowego

Kolejną istotną zmianą, związaną z budową sieci 5G, jest ułatwienie wdrażania punktów dostępu bezprzewodowego o bliskim zasięgu. Dyrektywa zapewnia, że lokowanie takich punktów będzie uniezależnione od lokalnych, indywidualnych pozwoleń, a wszelkie powody ograniczające ich lokowanie będą uzgodnione na poziomie krajowym. W połączeniu z przepisami mówiącymi o udostępnieniu operatorom przez publiczne organy wszystkich szczebli infrastruktury technicznej, takiej jak latarnie czy billboardy, daje to znaczące ułatwienia w budowie sieci opartych o wiele nadajników o małych zasięgach[19]. W przypadku sieci 5G, w oparciu o tego typu punkty dostępu, oferowane będą zapewne usługi wymagające bardzo dużej przepustowości, dla bardzo wielu użytkowników jednocześnie oraz związane z infrastrukturą inteligentnych miast.

Prawa użytkowników końcowych

W obszarze praw użytkowników końcowych kluczowe zmiany związane są z nowymi definicjami usług wchodzących w zakres usług łączności elektronicznej. Dotychczas regulacje były ściśle powiązane z charakterem sieci – tj. usługa łączności elektronicznej była definiowana jako usługa polegająca na przekazywaniu sygnałów w sieciach łączności elektronicznej – czyli wykluczała wszelkie usługi służące komunikacji, ale nieoparte o kontrolę sieci, czyli na przykład świadczone przez internet. Definicje zawarte w Kodeksie wyodrębniają w ramach usługi łączności elektronicznej następujące usługi[20]:

- usługę dostępu do internetu (zdefiniowaną w rozporządzeniu 2120/2015),
- usługę łączności interpersonalnej,
- usługę M2M (*machine to machine*) oraz nadawania (czyli usługi polegające całkowicie lub częściowo na przekazywaniu sygnałów).

Usługi łączności interpersonalnej

Wprowadzenie definicji usługi łączności interpersonalnej[21] ma na celu włączenie w zakres regulacji wszystkich usług zapewniających podobną funkcjonalność – takich jak połączenia głosowe realizowane przez sieć telefoniczną i przez internet, SMS, komunikatory, VOiP i podobne. Usługa ta dzieli się dodatkowo na[22]:

- usługę łączności interpersonalnej wykorzystującą numery,
- usługę łączności interpersonalnej niewykorzystującą numerów.

W uproszczeniu wszystkie usługi, które pozwalają na przekazanie informacji lub połączenie się z numerem z publicznych zasobów numeracji, wpadają do pierwszej definicji. Natomiast te, w których komunikacja odbywa się niezależnie od numeru telefonu – do drugiej. Przykładem pierwszej usługi jest SMS lub Skype, drugiej Messenger lub WhatsApp.

[13] *Art. 35*
[14] *Art. 49*
[15] *Art. 114 ustawy Prawo Telekomunikacyjne*
[16] *Art. 54*
[17] *Art. 4*
[18] *Art. 53.*
[19] *Art. 57*
[20] *Art. 2(4)*
[21] *Art. 2(4)*
[22] *Art.. 2(6) i Art. 2 (7)*

Rozróżnienia te są kluczowe nie tylko dla zrozumienia regulacji Kodeksu, ale także innych regulacji z tego obszaru (jak, chociażby rozporządzenia ePrivacy) oraz kierunku zmian regulacyjnych w obszarze cyfrowym. Dotychczas usługa typu SMS była objęta zupełnie innymi regulacjami niż usługi komunikatorów internetowych, mimo że z punktu widzenia użytkownika różnica między nimi nie była aż tak istotna. Co więcej, część komunikatorów oferowała połączenia na numery z publicznych zasobów numeracji, a nie tylko wewnątrz grona własnych użytkowników, natomiast nie obowiązywały ich przepisy np. o konieczności zapewnienia łączności alarmowej.

Stworzenie spójnych i przejrzystych regulacji w obszarze praw użytkowników końcowych bardzo utrudniały różnice techniczne i biznesowe pomiędzy poszczególnymi usługami. I tak na przykład **wymogi informacyjne**[23] (w tym nowy obowiązek dostarczenia użytkownikowi streszczenia umowy) zostały nałożone na wszystkie usługi oprócz M2M **Wymogi dotyczące przejrzystości ofert**[24] – na usługi dostępu do internetu i usługi łączności interpersonalnej.

W ramach przejrzystości ofert użytkownicy mają też mieć dostęp do porównywarki ofert. Porównywarką objęte mają być:

- usługi dostępu do internetu,
- usługi wykorzystujące numery,
- usługi niewykorzystujące numerów, które oparte są o taryfy lub stałe opłaty.

Obowiązki przedstawiania informacji odnośnie do jakości usługi[25] dotyczą usługi dostępu do internetu oraz usług łączności interpersonalnej, ale tylko w tym zakresie, w jaki kontrolują one elementy sieci. **Ograniczenie długości umowy do 24 miesięcy**[26] dotyczy wszystkich usług poza M2M i usługami niewykorzystującymi numeracji. Wreszcie, **obowiązek bezpłatnego łączenia z centrum powiadamiania ratunkowego**[27] i numerem 112 dotyczy usług wykorzystujących numery, ale tylko tych, z których można połączyć się z numerami z publicznego planu numeracji. Trzeba też zaznaczyć, że mikroprzedsiębiorstwa świadczące usługi łączności interpersonalnej niewykorzystujące numerów są całościowo wyłączone z przepisów tej części Kodeksu[28].

Czynniki komplikujące stosowanie przepisów dotyczących ochrony użytkownika końcowego

Jak widać, niemal każdy przepis dotyczący relacji między użytkownikiem końcowym a usługodawcą odnosi się do innego zakresu podmiotów. Częściowo wynika to z **różnic na poziomie technologii** (jak np. możliwość kontrolowania sieci, w której ma miejsce transmisja), częściowo ze **specyfiki modeli biznesowych** (np. komunikatory są najczęściej bezpłatne, nie wiążą użytkownika umowami na czas określony). Przepisy są dodatkowo komplikowane **przez rozszerzenie zakresu podmiotów objętych ochroną o mikro, małych i średnich przedsiębiorców** oraz organizacje non-profit. Ta grupa przedsiębiorców objęta jest prawem do informacji (tj. usługodawca ma obowiązek przekazać takie same informacje jak dla użytkowników indywidualnych), a także ograniczeniami co do czasu trwania umowy i przepisami dotyczącymi usług wiązanych[29]. Wprowadzona została opcja opt-out, tj. użytkownicy z tej grupy mogą samodzielnie z tych praw zrezygnować.

Trzecim czynnikiem komplikującym wdrażanie i stosowanie przepisów dotyczących ochrony użytkownika końcowego jest **poziom harmonizacji**[30]. Z jednej strony Kodeks przewiduje harmonizację maksymalną (tj. państwa członkowskie nie mogą stosować bardziej ani mniej restrykcyjnych przepisów) w obszarze praw użytkownika końcowego, z drugiej od tego generalnego zapisu jest szereg wyjątków. I tak, państwa mogą:

- rozszerzyć obowiązki informacyjne w przypadkach nieuregulowanych w Kodeksie oraz na nowe kwestie[31];
- mogą decydować, czy wymagać od usługodawców przekazywania informacji użyteczności publicznej[32];
- mogą też wprowadzać krótsze maksymalne okresy zobowiązania umownego[33];
- mogą rozszerzyć zakres przepisów stosowanych do umów wiązanych[34].

W rezultacie działalność firm oferujących usługi łączności elektronicznej na jednolitym rynku europejskim może być utrudniona – firmy te nie tylko będą musiały precyzyjnie orientować się we włączeniach i wyłączeniach podmiotowych dla poszczególnych przepisów, ale także śledzić rozwiązania wprowadzane w poszczególnych krajach i odpowiednio modyfikować swoją usługę.

Jedną z cech odróżniających tradycyjne usługi łączności elektronicznej od różnego rodzaju komunikatorów jest interoperacyjność. Możliwość połączenia się z innymi użytkownikami publicznych sieci jest zagwarantowana prawnie. Natomiast w przypadku komunikatorów, w większości przypadków łączność można nawiązać jedynie z innymi użytkownikami tej samej aplikacji. Ten problem był sygnalizowany w trakcie prac nad Kodeksem. W efekcie **Kodeks przewiduje szczególną procedurę nałożenia obowiązku interoperacyjności również na usługi łączności interpersonalnej niewykorzystujące numerów**. Może to jednak mieć miejsce dopiero po stwierdzeniu znacznego zagrożenia w łączności koniec-koniec w całej Unii, lub przynajmniej w trzech krajach członkowskich, oraz po konsultacjach Komisji z BEREC i wydaniu przez Komisję aktów delegowanych odnośnie do zakresu możliwych do nałożenia obowiązków[35].

[23] *Art. 102*
[24] *Art. 103*
[25] *Art. 104*
[26] *Art. 105*
[27] *Art. 109*
[28] *Art. 98*
[29] *Art. 102, Art. 105, Art. 102*
[30] *Art. 101*
[31] *Art. 102 (7)*
[32] *Art. 103 (4)*
[33] *Art. 105 (1)*
[34] *Art. 107 (5)*
[35] *Art. 59*

Przegląd przepisów dotyczących użytkowników końcowych

Cały zakres przepisów dotyczących praw użytkowników końcowych podlega też specjalnej procedurze przeglądowej[36]. Do 21 grudnia 2021 roku (trzy lata od przyjęcia Kodeksu, rok od daty transpozycji) BEREC ma obowiązek publikacji opinii w sprawie rozwoju rynku i adekwatności regulacji kodeksowych. Kolejne takie opinie będą publikowane co trzy lata lub na wniosek przynajmniej dwóch państw członkowskich. W rezultacie takiej opinii, oceniającej na ile regulacje usług łączności elektronicznej są odpowiednie dla realizacji celów całej dyrektywy, Komisja Europejska publikuje własne sprawozdanie oraz może wystąpić z wnioskiem legislacyjnym w sprawie zmiany tej części Kodeksu. Przegląd ten ma obejmować między innymi kwestie interoperacyjności w kontekście skutecznego dostępu użytkowników do służb ratunkowych, możliwości dokonywania swobodnych i świadomych wyborów przez użytkowników końcowych oraz wpływ przepisów na innowacje.

[36] *Art. 123*

Informacje o usługach niewykorzystujących numerów

Precyzyjne uchwycenie wpływu komunikatorów internetowych i innych usług OTT na rynek telekomunikacyjny było trudne również z powodu braku jasnej podstawy prawnej do zbierania o nich danych. Przykładowo, w przypadku analiz rynkowych NRA nie było możliwości dokładnej oceny konkurencji między SMSami a komunikatorami – a jest to istotny czynnik przy decydowaniu o wyznaczeniu operatora o pozycji znaczącej i nałożeniu bądź zdjęciu z niego obowiązków[37]. Podczas prac nad Kodeksem rozważano dwa rozwiązania tego problemu:

- **objęcie wszystkich usług łączności elektronicznej reżimem zezwolenia ogólnego**. Oznaczałoby to, że krajowe organy mogłyby żądać zgłoszenia każdego podmiotu świadczącego takie usługi do krajowego rejestru, wraz z podaniem podstawowego zakresu danych. **Ostatecznie pomysł ten upadł** – rejestr jest ograniczony do usług łączności elektronicznej innych niż usługi komunikacji elektronicznej niewykorzystujące numeracji[38].
- w to miejsce NRA, BEREC i inne właściwe organy zyskały **możliwość pozyskiwania wszystkich informacji niezbędnych do wykonywania zadań regulacyjnych**. Informacje te mogą być pozyskiwane nie tylko od przedsiębiorstw z sektora łączności elektronicznej, ale także z innych, ściśle powiązanych sektorów[39]. Wdrożenie tej zasady oznaczać będzie daleko idące poszerzenie wiedzy jaką będzie można pozyskać o nowoczesnych usługach i ich roli na rynku łączności elektronicznej. Poza wsparciem w analizie rynków i nakładaniu bądź zdejmowaniu obowiązków regulacyjnych może to też oznaczać generalnie lepsze zrozumienie zjawisk w gospodarce cyfrowej.

Infrastruktura

Obszar infrastruktury dotyczy w głównej mierze regulacji dostępu do sieci. W samej procedurze analizy rynków właściwych i oceny pozycji dominującej, ani też w zakresie możliwych do zastosowania środków zaradczych, nie zaszły rewolucyjne zmiany[40]. Kodeks przewiduje wydłużenie okresu analiz rynków właściwych z trzech do pięciu lat, zachowuje natomiast obowiązki dotyczące przejrzystości, niedyskryminacji, rozdzielności księgowej, dostępu do elementów sieci i urządzeń towarzyszących, a także kontroli cen. Nowym obowiązkiem, względem poprzedniego pakietu dyrektyw, jest

[37] *W Polsce rozwój komunikatorów internetowych był jednym z argumentów za deregulacją rynku zakańczania wiadomości SMS – https://archiwum.uke.gov.pl/koniec-regulacji-smsow-21306, natomiast analiza wydanych decyzji wskazuje, że UKE nie posiadał szczegółowej wiedzy na temat liczby wysyłanych wiadomości czy liczby użytkowników poszczególnych aplikacji, gdyż nie miał formalnej podstawy do żądania takich danych.*

[38] *Art. 12*

[39] *Art. 20*

[40] *Art. 63 – 74*

obowiązek dostępu do obiektów inżynierii lądowej i wodnej (np. budynków, słupów itp.). Z punktu widzenia Polski zmiana nie jest jednak rewolucyjna, gdyż podobny obowiązek występował już wcześniej w przepisach megaustawy[41].

Z budową i rozwojem infrastruktury wiążą się dwa inne, nowe przepisy, mogące mieć wpływ na rozwój sieci w Polsce. Przede wszystkim szczegółowo opisano proces i warunki dotyczące inwentaryzacji infrastruktury telekomunikacyjnej[42]. **Podmioty zobowiązane do sprawozdawania stanu posiadania będą odpowiadały materialnie za ewentualne nierzetelnie przekazane informacje**[43]. Brak możliwości sankcjonowania nierzetelnego działania w zakresie inwentaryzacji, np. w przypadku zgłoszenia infrastruktury w miejscu, gdzie się jej nie posiada i nie planuje zbudować lub odwrotnie, brak zgłoszenia istniejącej sieci, tworzyły w Polsce problemy związane z przyznawaniem pomocy publicznej na budowę nowych sieci. Z jednej strony zdarzały się przypadki, w których operator zgłaszał wiele terenów jako obszar swoich przyszłych inwestycji, przez co blokował możliwość objęcia ich programem pomocy publicznej. Z drugiej strony, niezgłoszona podczas inwentaryzacji infrastruktura mogła prowadzić do sytuacji, w której pomoc publiczna zostanie przyznana na obszarze, który powinien być z takiego wsparcia wykluczony. W myśl nowych przepisów, odpowiednie organy mogą, na podstawie informacji zebranych w ramach analizy geograficznej sieci szerokopasmowych, wyznaczyć obszary, na których takiej sieci nie ma i nie powstanie ona według planów inwestycyjnych operatorów. Na takich obszarach można zastosować pomoc publiczną lub zaoferować preferencyjne warunki jednemu z inwestorów. Takie preferencje występują w sytuacji, w której podmiot zgłosi się z deklaracją budowy sieci. Wtedy regulator (lub inny odpowiedni organ) może żądać od wszystkich innych operatorów powtórnej informacji o planach inwestycyjnych. Jeśli tym razem znów nikt nie przekaże informacji o planowanej inwestycji, podmiot deklarujący inwestycję ma gwarancję, że przez okres objętym prognozą będzie miał zapewniony lokalny monopol. Okres prognozy nie powinien przekroczyć trzech lat[44].

Drugim przepisem również nakierowanym bezpośrednio na wspieranie inwestycji jest **możliwość zwolnienia z części obowiązków regulacyjnych podmiotów o znaczącej pozycji rynkowej**[45]. Taki podmiot, planując budowę sieci światłowodowej, może wystąpić z otwartą ofertą współinwestycyjną – rozwiązanie to umożliwia innym operatorom współfinansowanie sieci oraz dzielenie ryzyka. Jeśli przynajmniej jedna taka umowa zostanie zawarta, regulator nie nakłada na ten podmiot innych obowiązków regulacyjnych. W zamyśle regulacje wypracowane w takim modelu mogą być łatwiejsze do zniesienia przez operatora, a zatem podnosić jego skłonność do budowy nowych sieci.

[41] *Ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych, Dz. U. 2010 Nr 106 z pózn. zm.*

[42] *Art. 22*

[43] *Art. 29*

[44] *Art. 22(2)-22(3), motyw 62*

[45] *Art. 76 i art. 79*

Usługa powszechna

Zmiany technologiczne i społeczne wpłynęły na znaczną część regulacji Kodeksu, a jednym z obszarów gdzie najwięcej przepisów uległo dezaktualizacji była usługa powszechna[46]. Stare regulacje przewidywały nie tylko możliwość wyłonienia operatora zapewniającego łączność telefoniczną (stacjonarną), ale także tworzenie spisu abonentów, zapewnienie budek telefonicznych czy biura numerów. Regulacja nie mówiła ani słowa o dostępie do internetu, nie brała też pod uwagę telefonii komórkowej. W Kodeksie wykreślono przepisy odwołujące się do nieaktualnych usług, jednak przede wszystkim wprowadzono wprost **obowiązek zapewnienia wszystkim konsumentom adekwatnego szerokopasmowego dostępu do internetu oraz do usług łączności głosowej** (a więc telefonii stacjonarnej bądź ruchomej)[47]. W szczególnych przypadkach, lub dla niektórych grup konsumentów, państwa członkowskie mogą też wprowadzić obowiązek stosowania specjalnych taryf socjalnych – w sytuacji, gdy ceny komercyjnie oferowanej usługi nie będą przystępne dla osób o niskich dochodach lub szczególnych potrzebach społecznych[48].

Należy przy tym zaznaczyć, że adekwatność usługi dostępu do internetu jest zdefiniowana nie parametrami przepustowości łącza, ale funkcjonalnie. Użytkownik musi być w stanie korzystać z minimalnego zestawu usług, obejmujących m.in. e-mail, handel i bankowość elektroniczną, sieci społecznościowe, komunikatory czy połączenia głosowe i wideo[49]. Wprowadzone zmiany dotyczą również sposobu finansowania kosztów netto usługi powszechnej. Koszty mogą być finansowane z budżetu państwa oraz ze specjalnego funduszu, który tworzyć będą wszyscy dostawcy usług łączności elektronicznej – a więc również dostawcy usług OTT takich jak komunikatory internetowe[50]. Poprzednie rozwiązania przewidywały jedynie fundusz sektorowy, a w związku z węższą definicją usług łączności elektronicznej, ograniczony był też zakres podmiotów obciążonych ewentualną składką.

Połączenia międzynarodowe

Na koniec warto wspomnieć o regulacji, która została zaproponowana przez Parlament Europejski w trakcie prac nad Kodeksem, jednak nie wynikała z wyjściowej propozycji Komisji Europejskiej. Rozwiązanie znacząco obniża ceny połączeń międzynarodowych. Przepisy obowiązują od 15 maja 2019 roku i obecnie za połączenia z Polski do innego kraju lub też SMS na unijny numer operator nie ma prawa naliczyć więcej niż 0,19 EUR za minutę rozmowy i 0,06 EUR za SMS. Jest to z pewnością jedno z rozwiązań najbardziej bezpośrednio dotykających konsumentów i w pewnym sensie uzupełnia wcześniejsze regulacje roamingowe[51].

[46] *Art. 84 i nast.*

[47] *Art. 84 (1)*

[48] *Art. 85*

[49] *Art. 84 (3), listę usług zawiera załącznik V do Kodeksu*

[50] *Art. 90*

[51] *Art. 50 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1971 z dnia 11 grudnia 2018 r. ustanawiające Organ Europejskich Regulatorów Łączności Elektronicznej (BEREC) oraz Agencję Wsparcia BEREC (Urząd BEREC), zmieniające rozporządzenie (UE) 2015/2120 oraz uchylające rozporządzenie (WE) nr 1211/2009.*

Wejście w życie

Państwa członkowskie mają dwa lata na implementację przepisów Kodeksu, czyli **do grudnia 2020 roku**[52]. Wyjątkiem jest wspomniana regulacja połączeń międzynarodowych, która została dodana do rozporządzania o BEREC wraz z datą wejścia w życie ustaloną na 15 maja 2019 r.[53] W Polsce wdrożenie Kodeksu będzie zapewne oznaczało bardzo daleko idące zmiany w ustawie Prawo telekomunikacyjne, a także w niektórych powiązanych aktach. Część prac jest już zaawansowana, projekt zmiany megaustawy został przyjęty przez Radę Ministrów, a zawiera między innymi przepisy dotyczące udostępniania infrastruktury na potrzeby małych komórek w sieciach 5G.[54]

Wbrew oczekiwaniom niektórych graczy rynkowych i daleko idącym propozycjom Komisji Europejskiej, Kodeks nie jest rewolucją i nie przewraca rynku telekomunikacyjnego do góry nogami. Jest jednak bardzo potrzebnym i istotnym dostosowaniem przepisów do obecnej sytuacji. W tym sensie buduje dobry fundament dla rozwoju rynku cyfrowego, wspierania konkurencyjności względem USA czy Chin i budowania nowoczesnej infrastruktury w Europie. Kluczowe pytanie jednak brzmi: czy wprowadzone zmiany będą wystarczające wobec tak szybko zmieniającego się rynku telekomunikacyjnego? Patrząc w nieco szerszym kontekście, odpowiedź nie jest jednoznaczna. To, co zapisano w Kodeksie, prawdopodobnie nie będzie wymagało bardzo szybkiej nowelizacji. Jednak najszybsze przemiany występują właśnie w obszarach, których Kodeks nie obejmuje, częściowo z definicji (jak na przykład dostęp do danych), a częściowo przez rozmyślne wyłączenie (jak ochrona prywatności). Kolejna tak obszerna Dyrektywa w obszarze telekomunikacyjnym w najbliższym czasie nam nie grozi, natomiast rewolucji należy się spodziewać z innych stron.

[52] *Art. 124*

[53] *Było to możliwe, gdyż zapisy rozporządzeń obowiązują bezpośrednio, a dyrektywa musi być dopiero implementowana do prawa krajowego*

[54] *https://legislacja.rcl.gov.pl/projekt/12318651*

Komentarz NASK

Europejski Kodeks Łączności Elektronicznej został przyjęty 11 grudnia 2018 roku. Jest to kompleksowa reforma regulacji telekomunikacyjnych (z 2009 roku) i jeden z istotniejszych projektów w zakresie Jednolitego Rynku Cyfrowego. Zmiany dotyczą dostępu do infrastruktury, regulacji widma radiowego oraz definicji i regulacji usług łączności elektronicznej.

Dyrektywa zwiększa także cyberbezpieczeństwo sektora telekomunikacyjnego. Zgodnie z art.40, operatorzy mają obowiązek zapewniania właściwych środków technicznych i organizacyjnych w razie wystąpienia zagrożenia dla bezpieczeństwa sieci lub usług. Środki te mają być proporcjonalne do istniejącego ryzyka, tak aby minimalizować skutki zagrożeń. Dodatkowo przedsiębiorcy zobowiązani są do zapewnienia integralności usług i informowania organów właściwych w przypadkach naruszeń bezpieczeństwa. Żeby określić jak istotny jest wpływ zagrożenia bezpieczeństwa, uwzględnia się w szczególności następujące parametry:

- liczbę użytkowników, których dotyczy incydent związany z bezpieczeństwem,
- czas trwania incydentu,
- geograficzny zasięg obszaru dotkniętego incydentem,
- zakres funkcjonowania sieci lub usługi,
- wpływ na działalność ekonomiczną i społeczną.

Parametry te są zgodne z tymi wprowadzonymi przez Dyrektywę NIS[55], a co za tym idzie, przez Ustawę o krajowym systemie cyberbezpieczeństwa[56].

Natomiast zgodnie z art. 41 Kodeksu właściwe organy krajowe mają prawo wymagać od przedsiębiorców:

- dostarczania informacji potrzebnych do oceny bezpieczeństwa i integralności ich usług i sieci, w tym dokumentów dotyczących polityki bezpieczeństwa;
- poddania się audytowi bezpieczeństwa przeprowadzanemu przez wykwalifikowany niezależny podmiot lub właściwy organ, a także udostępnienia właściwemu organowi wyników takiego audytu. Koszty audytu ponosi przedsiębiorstwo.

Równolegle w UE toczą się prace związane z siecią 5G. 26 marca Komisja Europejska wydała rekomendacje dotyczące działań i środków operacyjnych bezpieczeństwa sieci 5G w Unii Europejskiej.

Dokument wymienia konkretne środki operacyjne, które mają pomóc wypracować wspólne podejście państw członkowskich do kwestii bezpieczeństwa sieci 5G. Wdrożenie nowej sieci będzie wymagało specjalnych regulacji, a zwłaszcza spójnej polityki poszczególnych krajów w zakresie reagowania na incydenty. Dlatego KE przygotowała rekomendacje na poziomie europejskim i na poziomie krajów członkowskich.

Podstawowym narzędziem wsparcia we wprowadzeniu sieci 5G powinny być europejskie ramy certyfikacji cyberbezpieczeństwa. Ważną rolę odgrywać będzie również Grupa Współpracy[57], która przy udziale ENISA, stworzy zbiór narzędzi do reagowania na incydenty zagrażające bezpieczeństwu sieci. Toolbox ma pomóc zapewnić wysoki poziom ochrony danych i prywatności obywateli w całym cyklu sieci 5G.

PCz mają za zadanie ocenić ryzyka infrastruktury sieci 5G oraz przeprowadzić przegląd wymogów bezpieczeństwa.

W maju 2019 Rada Ministrów przyjęła projekt Ustawy o zmianie ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw. Założeniem tzw. „megaustawy" jest likwidacja barier administracyjno-prawnych hamujące rozwój infrastruktury telekomunikacyjnej. Ma ona ułatwić dotarcie z szybkim internetem tam, gdzie do tej pory było to nieopłacalne i trudne.

Najważniejsze kwestie zaadresowane w projekcie to:

- Rząd zdecydował się obniżyć pobierane od operatorów opłaty o 90%. Dzięki temu spadną koszty inwestycji.
- Zostanie powołany Fundusz Szerokopasmowy z rocznym budżetem ok. 140 mln. zł. Ma to pozwolić na dofinansowywanie budowy i rozwoju sieci telekomunikacyjnej.
- Prezes UKE będzie mógł zawierać z przedsiębiorcami telekomunikacyjnymi tzw. umowy zasięgowe, które zobowiążą operatorów do zapewnienia odpowiedniej jakości usług mobilnych nawet na tych obszarach, które określa się jako „trudne geograficznie".

[55] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Directive concerning measures for a high common level of security of network and information systems across the Union)*

[56] *Czytaj więcej o ustawie na stronie: https://cyberpolicy.nask.pl/ustawa-o-krajowym-systemie-cyberbezpieczenstwa/*

[57] *Mechanizm powołany na podstawie Dyrektywy NIS. Więcej na ten temat na stronie: https://cyberpolicy.nask.pl/grupa-wspolpracy/*

Paweł Kostkiewicz

Certyfikacja cyberbezpieczeństwa, czyli o co tak naprawdę chodzi?

Paweł Kostkiewicz – Kierownik Ośrodka Standaryzacji i Certyfikacji w NASK. Inżynier biocybernetyk i nauczyciel akademicki, odpowiedzialny za certyfikację cyberbezpieczeństwa w Państwowym Instytucie Badawczym NASK (tematy wiodące: Common Criteria, ISO/IEC 15408, ISO/IEC 18045, SOG-IS, CCRA, CyberSecurity Act, Dyrektywa NIS). Absolwent Wydziału Mechatroniki Politechniki Warszawskiej (magisterium z automatyki i robotyki, w specjalności biocybernetyka i inżynieria biomedyczna). Pracował w firmach i instytucjach w „złotym trójkącie": biznes-nauka-administracja. Doświadczenie gromadził jako kierownik specjalistycznych zespołów i architekt systemów teleinformatycznych – m.in. w kilku dużych projektach związanych z budowaniem systemów informatycznych dla rejestrów centralnych, wsparcia rządowego procesu legislacyjnego, zarządzania w publicznej opiece zdrowotnej, jak również budowy specjalistycznej infrastruktury teleinformatycznej tj. sieci rozległe i duże centra przetwarzania danych.

Obecnie rozwija w NASK Jednostkę Certyfikującą (Certification Body, jest również członkiem międzynarodowych grup roboczych związanych z certyfikacją cyberbezpieczeństwa (SOG-IS, CCRA).

Komentarz NASK

Od 27 czerwca br. obowiązuje Akt o Cyberbezpieczeństwie (Cybersecurity Act). Jest to druga, po dyrektywie NIS, ogólnoeuropejska regulacja w dziedzinie cyberbezpieczeństwa. CA składa się z dwóch części: nowego permanentnego mandatu dla ENISA oraz **rozporządzenia tworzącego europejskie ramy certyfikacji cyberbezpieczeństwa dla produktów i usług ICT.** Jest to bardzo istotna regulacja, która znacznie zmieni funkcjonujący obecnie model certyfikacji, zdominowany przez SOG-IS (Senior Official Group Information Security Systems)[58].

Rozporządzenie w sprawie certyfikacji cyberbezpieczeństwa to pierwsze prawo dotyczące rynku wewnętrznego, które odpowiada na potrzebę podniesienia poziomu bezpieczeństwa produktów, usług i procesów ICT. Stworzenie europejskich ram certyfikacji cyberbezpieczeństwa to przełomowy krok, który w efekcie umożliwi zniesienie barier, utrzymujących się na rynku cyfrowym.

Rozporządzenie wprowadza dobrowolną certyfikację produktów, usług i procesów ICT, a także w wybranych przypadkach, możliwość wprowadzenia obowiązkowej certyfikacji. Poza tym określa trzy poziomy bezpieczeństwa: podstawowy, istotny i wysoki. Państwa członkowskie mają także obowiązek powołania krajowych organów ds. certyfikacji cyberbezpieczeństwa.

Mimo, że rozporządzenia obowiązuje w sposób bezpośredni, to w Polsce konieczne będzie wprowadzenie nowych regulacji, ponieważ do tej pory nie funkcjonowała w naszym kraju certyfikacja cyberbezpieczeństwa[59].

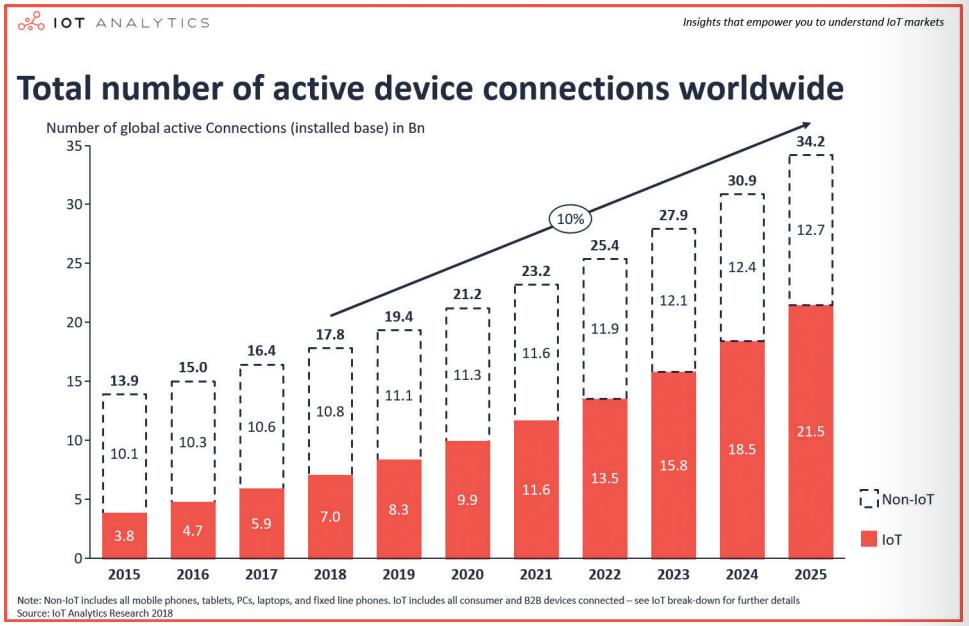
[58] *Porozumienie SOG-IS zostało zawarte w 1997 roku, w odpowiedzi na decyzję Rady UE z marca 1992 roku. Sygnatariusze porozumienia mogą samodzielnie oceniać i certyfikować produkty i usługi sektora IT, zgodnie z międzynarodową normą OSO/IEC 15408, która pozwala zweryfikować bezpieczeństwo systemów teleinformatycznych pod względem formalnym. Polska dołączyła do grupy państw sygnatariuszy porozumienia SOG-IS w 2017 roku.*

[59] *Więcej informacji na temat rozporządzenia dostępnych jest na stronie: https://cyberpolicy.nask.pl/akt-o-cyberbepzieczenstwie-certyfikacja-cyberbezpieczenstwa/*

Kontekst tworzenia certyfikacji ICT

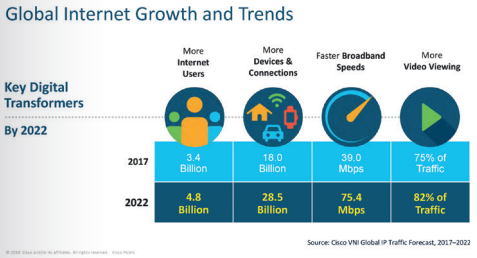
Według firmy Gartner, Inc. w 2017 roku do Internetu miało być podłączonych 8,4 miliarda urządzeń („connected things"). Prognozy mówią, że liczba ta osiągnie 20,4 miliarda do 2020 roku.

Portal „IoT Analytics" poinformował, że w 2017 roku używaliśmy 6 miliardów urządzeń IoT oraz ponad 16 miliardów urządzeń łącznie (wliczając komputery, telefony, tablety itp.).



Źródło: https://iot-analytics.com

Z kolei Visual Networking Index (VNI) firmy Cisco przewiduje, że do 2022 roku w globalnej sieci pojawi się więcej ruchu IP niż we wszystkich poprzednich "latach internetowych" łącznie (do końca 2016 r.). Innymi słowy w 2022 r. powstanie **więcej ruchu niż przez 32 lata** od uruchomienia Internetu! Skąd będzie pochodził ten ruch? Wygenerujemy go wspólnie, my wszyscy, nasze maszyny i zmieniający się sposób korzystania z Internetu. Do 2022 r. 60 proc. światowej populacji będzie użytkownikami globalnej sieci. Ponad 28 miliardów urządzeń i połączeń będzie dostępnych online. A transmisja wideo będzie stanowić 82% całego ruchu IP.



Źródło: Cisco Visual Networking Index (VNI)

Wiele wskazuje na to, że te i podobne prognozy inspirowały twórców nowego unijnego prawa. W pierwszym akapicie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych znajdujemy wyjaśnienie przyczyn podjęcia decyzji o wydaniu tego aktu:

„Sieci i systemy informatyczne oraz sieci i usługi łączności elektronicznej odgrywają kluczową rolę w społeczeństwie i stały się podstawą wzrostu gospodarczego. Technologie informacyjno-komunikacyjne (ICT) stanowią podstawę złożonych systemów wspierających codzienne działania społeczne, zapewniają funkcjonowanie naszej gospodarki w kluczowych sektorach, takich jak opieka zdrowotna, energetyka, finanse i transport, a zwłaszcza wspomagają funkcjonowanie rynku wewnętrznego. […]".

Wnioski z przytoczonych wyżej prognoz mogą być rozmaite, ale jedno wydaje się pewne. Urządzenia pojawiają się, ponieważ chcemy tego my – użytkownicy. Czasem nie mamy świadomości, że chcąc wiedzieć i widzieć więcej, powodujemy gwałtowne mnożenie się urządzeń, czujników, połączeń w sieci, nieustannie aktywnych aplikacji itd. Chcemy więcej komfortu, informacji, wiedzy. Otaczamy się technologią, która ułatwia nam życie codzienne i pracę. Te potrzeby są zróżnicowane, od błahych po istotne. Od zawodowych po prywatne. Ale bez względu na potrzeby, chcemy, żeby to wszystko działało szybko (błyskawicznie!), **bardziej niezawodnie** niż cokolwiek innego. A przede wszystkim chcemy czuć się z technologią **bezpiecznie.**

Przypominają się tutaj słowa wielkiego futurysty Artura C. Clarka, o tym, że „każda wystarczająco zaawansowana technologia jest nieodróżnialna od magii". Podsumowując, nie wiemy i nie bardzo chcemy wiedzieć, jak to działa, ale chcemy mieć przekonanie, że działa właściwie i dobrze dla nas. Bezpieczeństwo każdy z nas zapewne postrzega odrobinę inaczej, ale można zgodzić się w sprawach podstawowych, takich jak niezawodność czy przewidywalność. Czujemy się bezpiecznie – większość z nas – kiedy sprawy dzieją się „tak jak powinny". A zatem chcemy więcej urządzeń, szybszych i bezpieczniejszych.

Rozporządzenie stanowi, że „Europejskie certyfikaty cyberbezpieczeństwa i unijne deklaracje zgodności powinny pomóc użytkownikom końcowym w dokonywaniu

świadomego wyboru. Dlatego też produktom ICT, usługom ICT i procesom ICT, które uzyskały certyfikację lub w przypadku których wydana została unijna deklaracja zgodności, powinny towarzyszyć ustrukturyzowane informacje dostosowane do zakładanego poziomu wiedzy technicznej przewidywanych użytkowników końcowych. Wszystkie takie informacje powinny być dostępne on-line, a w stosownych przypadkach – w postaci fizycznej." (wstęp pkt. 93).

Certyfikacja, czyli budowanie zaufania do technologii

Filarem zaufania i podstawą wyboru jest rekomendacja autorytetu, któremu ufamy. Czy da się rolę autorytetu ująć, określić, zaprogramować do działania systemowo? Czytamy w Rozporządzeniu *Cybersecyrity Act:* „Ustanawia się **europejskie ramy certyfikacji cyberbezpieczeństwa** w celu poprawy warunków funkcjonowania rynku wewnętrznego poprzez zwiększenie poziomu cyberbezpieczeństwa".

W świecie techniki stosuje się powszechnie mechanizmy kontroli jakości, dozoru technicznego, atestacji czy wzorcowania. Nie zaskakuje nas, że waga w sklepie działa prawidłowo i niemal idealnie zbieżnie z innymi, nie dziwi znak atestacyjny na takich urządzaniach jak gaśnice czy windy. Przeciwnie, intuicyjnie i podświadomie wiemy, że za tym przewidywalnym sposobem działania stoi systemowe rozwiązanie – waga podlega wzorcowaniu, a windy przeglądom i okresowej kontroli. To efekty działania „systemów oceny zgodności" zapewniających odpowiednią jakość (sprawność, wydajność, dokładność) urządzeń.

Czy mamy podobny komfort użytkowania rozwiązań z dziedziny IT? Większość z nas odpowie, że zdarza się (często?) narzekać na wydajność czy nieprzewidywalne zachowanie komputera lub telefonu. Znajomo wydają się brzmieć zwroty takie jak „to chyba jakiś wirus" lub „coś go zamula".

I tutaj nasuwa się refleksja – jak to możliwe, że nie poddajemy właściwie żadnym cyklicznym kontrolom czy testom urządzeń, których używamy nawet kilkaset razy dziennie (telefon) i przez wiele godzin w tygodniu (komputer)? A jednocześnie powierzamy tym urządzeniom swoje dane osobowe, informacje wrażliwe, transakcje finansowe, sekrety zawodowe i prywatne. Gaśnicę, której zapewne nigdy nie użyjemy, oddajemy do sprawdzenia minimum raz do roku. Tymczasem na powtarzające się prośby programu antywirusowego o uruchomienie skanowania i monity systemu operacyjnego o aktualizację staramy się odpowiadać jak najdłużej „odłóż to na później".

Certyfikat bezpieczeństwa informatycznego – magiczny amulet

Chcielibyśmy, żeby urządzenia ze świata IT były **„bezpieczne"**. Żeby smartfon nie kradł danych, żeby kamerka nie podglądała, żeby serwer odpierał ataki hackerów, żeby sieć naszej firmy nie zatykała się pod wpływem złośliwego ruchu, żeby nasz ulubiony program pocztowy obronił nas przed oszustami, którzy próbują wyłudzić pieniądze lub dane. A najprościej mówiąc, chcielibyśmy, żeby dało się w miarę jasny sposób stwierdzić, że kupujemy produkty lub używamy usług IT, które są bezpieczne. Można powiedzieć, że bezpieczny smartfon, komputer albo usługa w chmurze – to jest dokładnie to czego oczekujemy. Jakkolwiek eksperci dookreślą czym jest cyberbezpieczeństwo, dla nas – użytkowników – to ma być pewność, że świat IT, który nas otacza jest bezpieczny.

W świecie idealnym, zamawiając usługę czy kupując produkt, moglibyśmy sprawdzić czy jest to rozwiązanie cyberbezpieczne, a na pudełku lub w opisie byłoby napisane po prostu „jesteś bezpieczny". **Certyfikacja cyberbezpieczeństwa** stanowi właśnie odpowiedź na tą potrzebę. W preambule do najnowszego rozporządzenia Cybersecurity Act możemy przeczytać:

„Certyfikacja cyberbezpieczeństwa odgrywa ważną rolę, jeżeli chodzi o zwiększanie zaufania do produktów ICT, usług ICT i procesów ICT oraz ich bezpieczeństwa. Jednolity rynek cyfrowy, a w szczególności gospodarka oparta na danych i internet rzeczy, mogą się prawidłowo rozwijać jedynie w atmosferze ogólnego publicznego zaufania, że takie produkty, usługi i procesy zapewniają konkretny poziom cyberbezpieczeństwa. Połączone z siecią i zautomatyzowane pojazdy, elektroniczne wyroby medyczne, systemy sterowania automatyki przemysłowej oraz inteligentne sieci stanowią tylko niektóre przykłady sektorów, w których certyfikacja jest już szeroko stosowana lub najprawdopodobniej będzie stosowana w najbliższej przyszłości".

Natomiast w komunikacie z roku 2016 „Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego" Komisja Europejska przedstawiła „potrzebę wysokojakościowych, dostępnych cenowo i interoperacyjnych produktów i rozwiązań w dziedzinie cyberbezpieczeństwa. Podaż produktów, usług i procesów ICT na jednolitym rynku nadal charakteryzuje się dużym rozdrobnieniem pod względem geograficznym. Do luk mających wpływ na jednolity rynek w dziedzinie cyberbezpieczeństwa należy m.in. brak interoperacyjnych rozwiązań (norm technicznych), praktyk i ogólnounijnych mechanizmów certyfikacji. Komisja podkreśliła zapotrzebowanie na bezpieczne podłączone do sieci produkty i systemy oraz

wskazała, że ustanowienie europejskich ram bezpieczeństwa ICT określających **zasady certyfikacji bezpieczeństwa** ICT w Unii mogłoby zarówno podtrzymać zaufanie do Internetu, jak i przeciwdziałać obecnemu rozdrobnieniu rynku wewnętrznego[60].

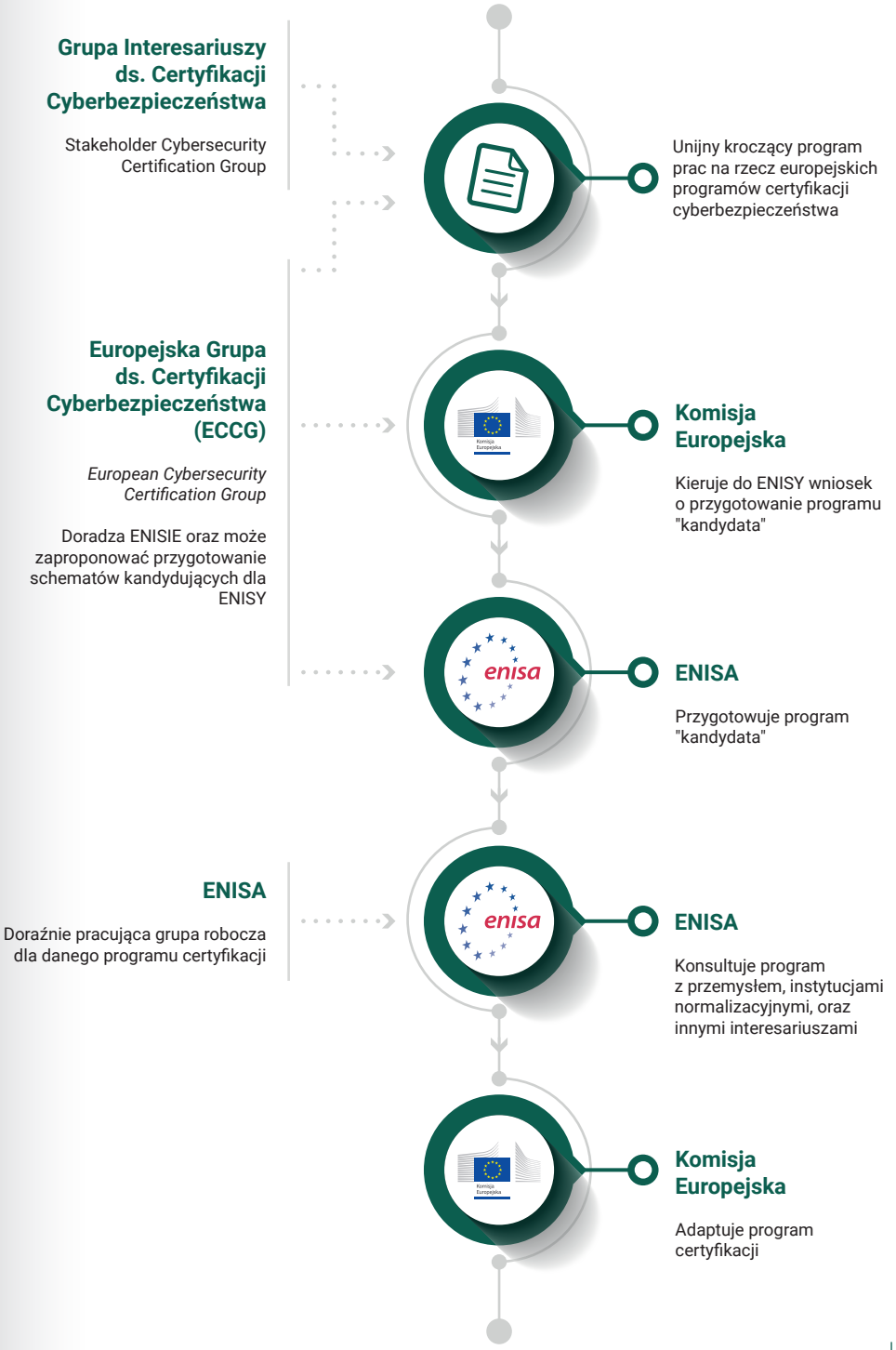
Certyfikat. Dobrze… i co dalej?

Certyfikacja jest tylko jednym z elementów (etapów) działającego systemu oceny zgodności. Z pewnością ważnym, często kluczowym dla producenta, ponieważ umożliwia np. wejście na rynek krajowy czy sprzedaż w określonej branży. Pamiętajmy przy tym, że wydanie certyfikatu (decyzji atestacyjnej) bez wdrożonych mechanizmów kontrolnych nie zapewni utrzymania jakości w czasie użytkowania (stałości cech). Do tego potrzebne są **„mechanizmy służące wykazaniu ciągłej zgodności z określonymi wymogami[61]”.**

Cykliczny i systematyczny reżim kontroli dotyczy w największym stopniu urządzeń przemysłowych, takich jak windy, dźwigi czy maszyny w ciągach produkcyjnych. Jakość działania np. dokładność wskazań instrumentów pomiarowych (pomimo wydanego certyfikatu) nie jest dana „na zawsze”. Na skutek starzenia się elementów mechanicznych i elektronicznych, zmian warunków użytkowania i otoczenia oraz wielu losowych czynników, działanie urządzenia ulega zmianom, z reguły na gorsze. Z tego powodu wprowadzono obowiązek stałego dozoru technicznego, monitorowania parametrów, kontroli jakości. Znacznie trudniej wprowadzić takie mechanizmy do urządzeń przeznaczonych na rynek powszechny, czyli dla konsumentów indywidualnych.

Artykuł 54 Rozporządzenia (UE) 2019/881 – wszystko co najważniejsze

Jak w praktyce realizować certyfikację cyberbezpieczeństwa wyjaśnia w dużej mierze art. 54 Rozporządzenia. To kluczowy fragment aktu prawnego, który precyzyjnie formułuje oczekiwania wobec **europejskich programów certyfikacji.** Program certyfikacji to „kompleksowy zbiór przepisów, wymogów technicznych, norm i procedur ustanowionych na poziomie unijnym i mających zastosowanie do certyfikacji lub oceny zgodności określonych produktów ICT, usług ICT i procesów ICT”.



[60] *https://cyberpolicy.nask.pl/wzmacnianie-europejskiego-systemu-odpornosci-cybernetycznej-oraz-wspieranie-konkurencyjnego-i-innowacyjnego-sektora-bezpieczenstwa-cybernetycznego/*

[61] *Art. 54 Rozporządzenia o ENISA i certyfikacji cyberbezpieczeństwa.*

W artykule „Rozporządzenie w sprawie certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjnych i komunikacyjnych" opisano mechanizm proponowania (zgłaszania), następnie opracowywania (istotna odpowiedzialność spada tutaj na pracowników ENISA), a w konsekwencji ogłoszenia (przez Komisję Europejską) europejskiego programu certyfikacji. Podstawą każdego programu muszą być normy i wymogi techniczne.

Inne ważne elementy każdego z programów certyfikacji to m.in.

- jasna deklaracja co do *rodzaju lub kategorii objętych danym programem produktów ICT, usług ICT i procesów ICT;*
- wskazanie, czy w ramach systemu *dozwolona jest ocena zgodności przez stronę pierwszą* (innymi słowy czy istnieje możliwość oceny zgodności przez producenta);
- *szczegółowe kryteria oceny i metody, w tym rodzaje oceny* (co ma zapewnić m.in. obiektywizm i porównywalność wyników oceny).

A także kluczowe mechanizmy, które powinny zapewnić jakość certyfikowanych produktów w czasie ich używania:

- *zasady monitorowania zgodności produktów ICT, usług ICT i procesów ICT […] w tym mechanizmy służące wykazaniu ciągłej zgodności z określonymi wymogami cyberbezpieczeństwa;*
- *warunki […] utrzymywania, kontynuowania i odnawiania europejskich certyfikatów cyberbezpieczeństwa, a także warunki rozszerzania lub ograniczenia zakresu certyfikacji;*
- *zasady dotyczące skutków dla produktów ICT, usług ICT i procesów ICT, które uzyskały certyfikację lub w przypadku których wydana została unijna deklaracja zgodności, które jednak nie spełniają wymogów programu;*
- *zasady dotyczące sposobu zgłaszania uprzednio niewykrytych, a wpływających na cyberbezpieczeństwo podatności produktów ICT, usług ICT i procesów ICT oraz sposobu postępowania z nimi.*

Normy a sprawa cyberbezpieczeństwa

Niezależnie od czego zaczną dyskusję eksperci **na temat norm cyberbezpieczeństwa,** za rogiem zawsze stoi i spokojnie czeka na przywołanie do tablicy norma zwana nieco tajemniczo **„Common Criteria".**

Jest to jedna z najszerzej stosowanych specyfikacji w zakresie oceny i certyfikacji produktów teleinformatycznych. Nazwa „wspólne kryteria" dotyczy połączenia i ujednolicenia trzech opracowań normalizacyjnych:

- **ITSEC** – norma opracowana w Europie (przez Francję, Niemcy, Holandię i Wielką Brytanię),
- **CTCPEC** – norma kanadyjska bazująca na opracowaniach amerykańskiego Departamentu Obrony,
- **TCSEC** – norma amerykańska (DoD 5200.28 Std) zwana potocznie „the Orange Book".

Warto sobie również uświadomić związek pomiędzy certyfikacją cyberbezpieczeństwa a bezpieczeństwem państwa, np. pod kątem zapewnienia ciągłości świadczenia usług kluczowych w szczególnie wrażliwych sektorach gospodarki, jak finanse, energetyka czy zdrowie.

Czym jest Common Criteria?

Obecnie *Common Criteria* (dostępna również jako norma ISO 15408) to zestaw trzech dokumentów głównych (rozdziałów), który jest wspomagany dokumentem metodologicznym „Common Methodology for Information Technology Security Evaluation"- inaczej **CEM**. Norma *Commmon Criteria* została opublikowana po raz pierwszy w roku 1993. Od tego momentu jest stale monitorowana, aktualizowana i rozwijana, co owocuje publikacją kolejnych edycji („versions") i rewizji („revisions").

Aktualny na dzień pisania tekstu (lipiec 2019) jest dokument w wersji nr 3.1 – rewizja nr 5, datowany na kwiecień 2017. Ciekawym i wartym odnotowania jest fakt, że norma *Common Criteria* jest opracowywana wspólnym wysiłkiem specjalistów z organizacji kilkunastu krajów świata. Specyficzne dla normy jest również to, że autorzy udzielają licencji międzynarodowym organizacjom standaryzującym (ISO i IEC), które następnie publikują normy rodziny ISO/IEC 15408 (części -1, -2 i -3) zawierające ekwiwalent Common Criteria i odpowiednio ISO/IEC 18045 dla dokumentu CEM.

Na terenie Polski normy ISO/IEC 15408:1-3 i 18408 są przyjęte do stosowania w wersji anglojęzycznej i dostępne z sygnaturą PN-ISO/IEC 15408-1:2016-10. Zainteresowanych stosowaniem norm zachęcam do korzystania z darmowych wersji źródłowych (dostępnych na portalu http://commoncriteriaportal.org).

Common Criteria jest standardem dotyczącym zagadnień bezpieczeństwa, a w szczególności oceny bezpieczeństwa szeroko rozumianej teleinformatyki. Ocenie i certyfikacji podlegać mogą fizyczne urządzenia oraz oprogramowanie (firmware i software), jak również kombinacje obu. Produkty certyfikowane opatrzone są logotypem przedstawionym na rysunku poniżej.

Certyfikacja cyberbezpieczeństwa – co z tego wynika dla Polski?

NASK uruchomił Jednostkę Certyfikującą (*Certification Body*), która będzie wydawała certyfikaty cyberbezpieczeństwa. Głównym kierunkiem prac, które obecnie prowadzimy w Instytucie, jest przygotowanie zdolności do wydawania certyfikatów w oparciu o normę *Common Criteria*. Pierwsze ważne i realne działania w tym kierunku mamy już za sobą. W szczególności podpisaliśmy, działając w oparciu o pełnomocnictwo Ministerstwa Cyfryzacji, dwie umowy (porozumienia SOG-IS i CCRA) o wzajemnym, międzynarodowym uznawaniu certyfikatów wydanych przez odpowiednie instytucje m.in. z USA, Niemiec i Francji. W praktyce oznacza to, że już teraz mamy w Polsce narzędzie i podstawę do uznawania certyfikatów wydanych w krajach uczestniczących w tych porozumieniach.

W pragmatyce zakupów publicznych (specyfikacji przedmiotowych) już teraz jest czas i miejsce na odwołanie do tych certyfikatów. Do końca 2019 roku rozpoczniemy pierwsze pilotażowe certyfikacje, a w pierwszym kwartale 2021 roku powinniśmy osiągnąć pełną sprawność operacyjną. Polskich producentów ICT (sprzętu i oprogramowania) zainteresowanych pilotażową certyfikacją ich wyrobów zapraszamy do kontaktu: certification@nask.pl.

Warto w tym miejscu zaznaczyć, że program certyfikacji oparty o *Common Criteria* będzie najprawdopodobniej **pierwszym europejskim programem certyfikacji cyberbezpieczeństwa** zatwierdzonym i ogłoszonym przez Komisję Europejska. Prace w tym kierunku są bardzo zaawansowane.

Certyfikacja cyberbezpieczeństwa – czy to się uda…

W najbliższym czasie możemy spodziewać się intensywnego zainteresowania grup producentów oraz regulatorów rynku w krajach członkowskich tematem opracowywania nowych europejskich programów certyfikacji. Wydaje się jednak, że postulat popularyzacji certyfikacji na rynku wspólnym zapisany w *Rozporządzeniu* będzie możliwy do spełnienia wyłącznie w przypadku realnego zainteresowania odbiorców (konsumentów).

Innymi słowy, popularność certyfikatów cyberbezpieczeństwa zależy od nas, kupujących, projektujących, wdrażających systemy ICT. Jeżeli pojawi się zauważalny popyt na produkty certyfikowane, to z pewnością europejskie ramy certyfikacji cyberbezpieczeństwa dają szansę na stworzenie programów certyfikacji, które na ten popyt odpowiedzą. Osobną i bardzo istotną kwestią będzie dyskusja nt. obowiązkowej certyfikacji. W Rozporządzeniu określono obowiązek przeglądu zasad certyfikacji cyberbezpieczeństwa w kierunku określenia obowiązku certyfikacji dla wybranego zakresu przedmiotowego (produktów, usług). W obecnej fazie obowiązywania nowego rozporządzenia certyfikacja jest dobrowolna. Zatem: certyfikować czy nie certyfikować? Na razie nie ma przymusu, a decyzja jest w naszych rękach.

Dr Adam Kozakiewicz

Projekt SISSDEN czyli badawczo-rozwojowa odpowiedź na rosnące potrzeby tworzenia pełnej świadomości sytuacyjnej

Dr Adam Kozakiewicz – kierownik Zakładu Metod Bezpieczeństwa Sieci i Informacji w PIB NASK, gdzie odpowiada za projekty naukowo-badawcze w obszarze cyberbezpieczeństwa. W 2008 roku otrzymał stopień naukowy doktora nauk technicznych w specjalności Telekomunikacja na Politechnice Warszawskiej. Rozprawa doktorska Effective Bandwidth Theory for Pricing and QoS Control of Computer Networks koncentrowała się na zagadnieniach modelowania ruchu w sieciach telekomunikacyjnych. Wykaz jego publikacji obejmuje kilkadziesiąt artykułów naukowych.

Wraz z rozwojem społeczeństwa informacyjnego następuje coraz większe uzależnienie od połączonych systemów informatycznych. Najważniejsze sektory gospodarki, takie jak energetyka, finanse czy zdrowie, opierają się na złożonych systemach teleinformatycznych. Również nasze codzienne życie stało się zależne od nowoczesnych technologii. Jednocześnie systemy teleinformatyczne są coraz podatniejsze na ataki internetowe. Indywidualna ochrona poszczególnych systemów, oparta na analizie odbieranych i wysyłanych komunikatów, nie jest już wystarczająca. Potrzebne są nowe, holistyczne podejścia, biorące pod uwagę informacje zebrane z wielu różnych źródeł, które zapewniają lepsze zrozumienie intencji atakujących, ich metod i możliwości, a także ewolucji czynników ryzyka.

Wobec coraz bardziej zaawansowanych i zorganizowanych zagrożeń oraz rosnącego poziomu złożoności użytkowanych sieci i systemów, podstawą obrony staje się posiadanie odpowiedniej świadomości sytuacyjnej. Ilość, jakość i aktualność informacji wykorzystywanych do przeciwdziałania zagrożeniom, decyduje o możliwości skutecznej reakcji, zapobiegania i zwalczania internetowych zagrożeń. Tymczasem, jak potwierdzają raporty ENISA (EU Agency for Cybersecurity – Europejskiej Agencji ds. Cyberbezpieczeństwa), to właśnie w zakresie tych zdolności wśród europejskich podmiotów występują szczególnie niebezpieczne braki. Sieci są często bronione przy użyciu skutecznych narzędzi, jednak bez pełnej świadomości w zakresie rodzaju ataku, a więc bez możliwości skutecznego wykorzystania zabezpieczeń. To właśnie dlatego NASK PIB stworzył międzynarodowy projekt SISSDEN, będący badawczo-rozwojową odpowiedzią na rosnące potrzeby budowania świadomości sytuacyjnej.

Czym jest projekt SISSDEN?

W 2016 roku NASK po raz pierwszy w swojej historii przyjął rolę koordynatora dużego międzynarodowego projektu badawczo-rozwojowego w ramach programów ramowych Komisji Europejskiej. SISSDEN (Secure Information Sharing Sensor Delivery Event Network) to pierwszy wniosek składany przez NASK w nowym wówczas programie Horyzont 2020 – i od razu skuteczny.

Celem projektu jest poprawa cyberbezpieczeństwa europejskich jednostek i użytkowników poprzez rozwój świadomości sytuacyjnej i współdzielenie informacji o zagrożeniach. Zadania podjęło się koordynowane przez NASK konsorcjum ośmiu jednostek europejskich, w tym zarówno dużych firm (niemiecki Deutsche Telekom, włoska Poste Italiane), małych i średnich przedsiębiorstw (francuski Montimage, brytyjski Cyberdefcon, szwajcarski Eclexys), fundacji non-profit (holenderski Shadowserver[62] – europejski oddział amerykańskiej fundacji) jak i jednostek badawczych (NASK, niemiecki Universität des Saarlandes). Budżet

[62] *https://www.shadowserver.org/who-we-are/*

projektu znacznie przekroczył 6 milionów euro, a finansowanie zostało uzyskane w ramach grantu Komisji Europejskiej nr 700176.

Projekt zakończył się w kwietniu 2019 roku i możemy zaprezentować jego efekty. Artykuł prezentuje przede wszystkim te aspekty, w których NASK pełnił wiodącą rolę merytoryczną. Zakres całego projektu był natomiast o wiele szerszy.

Globalna sieć honeypotów

Podstawowym zadaniem SISSDENa była **budowa systemu zbierania informacji o zagrożeniach w skali globalnej**, wykorzystującego nowoczesne systemy pułapkowe (honeypoty), udające rzeczywiste usługi. Dzięki sieci honeypotów stworzono bogate i wiarygodne źródło informacji, które pozwala budować świadomość sytuacyjną na temat zagrożeń teleinformatycznych.

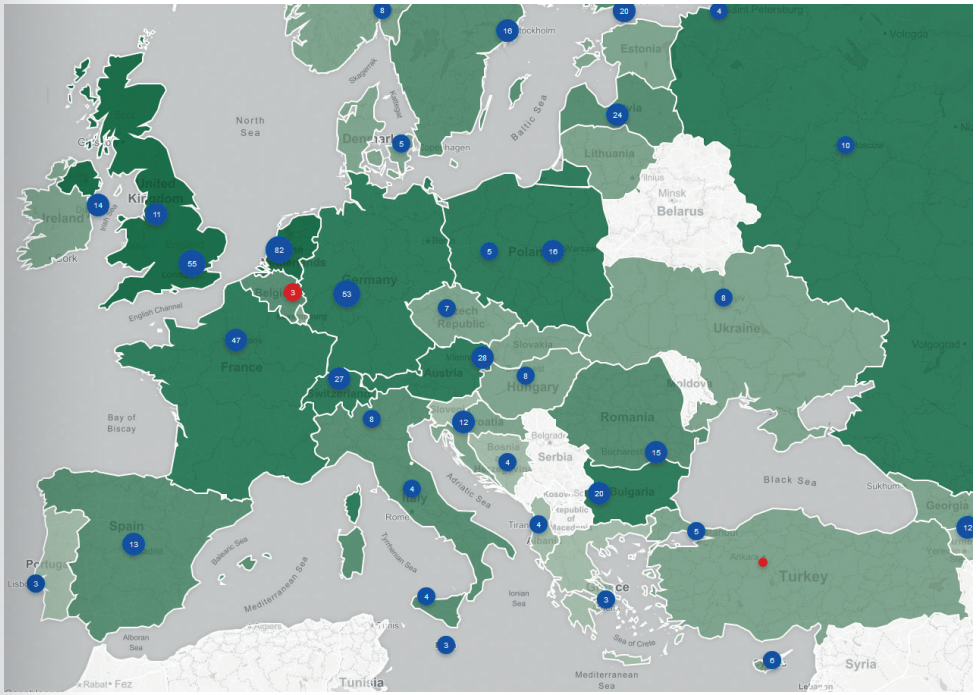
Honeypoty, jako symulowane usługi, są pasywnymi systemami obserwacyjnymi. Nie mają wglądu w rzeczywisty, codzienny ruch krążący w sieci, nie mogą też w niego ingerować – widzą tylko to, co zostało wysłane bezpośrednio do nich. Wielką zaletą takiego podejścia jest jego przejrzystość etyczna – cokolwiek trafia do honeypotu, z natury nie zawiera prywatnej korespondencji, wrażliwych informacji itp. Niemal wszystko, co widzą honeypoty, to działania z gruntu złośliwe, takie jak:

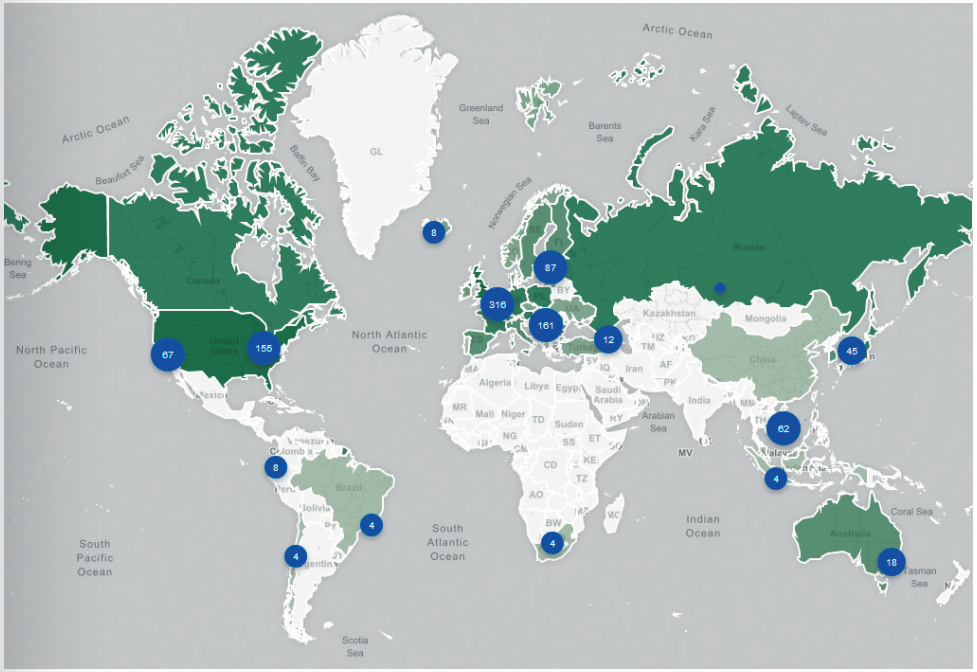
- ataki,
- poszukiwanie podatnych komputerów, które mogłyby być wykorzystane w botnecie,
- poszukiwanie usług możliwych do wykorzystania w charakterze nieświadomych „wzmacniaczy" w atakach odbiciowych.

Niewielka część obserwowanego ruchu to zasadniczo nieszkodliwe, ale i bezosobowe działania, takie jak globalne skany całego Internetu wykonywane przez różne jednostki w pozytywnych celach (np. badawczych lub informacyjnych).

W efekcie **SISSDEN jest w stanie obserwować na wielką skalę działanie różnych automatycznych i półautomatycznych zagrożeń.** Nie może jednak wykrywać (ani tym bardziej blokować) zagrożeń występujących w bezpośredniej, ukierunkowanej komunikacji istniejących serwisów. Możliwości reakcji na zidentyfikowane zagrożenia są więc ograniczone do ostrzegania odpowiedzialnych za daną sieć podmiotów.

W ramach projektu powstała globalna sieć ponad 250 czujników rozmieszczonych na całym świecie. Ponieważ każdy z czujników ma kilka adresów IP, sieć obserwacyjna składała się z blisko tysiąca adresów, pokrywających 119 systemów autonomicznych w 58 krajach – w tym wszystkich państwach członkowskich Unii Europejskiej. Poniższe grafiki przedstawiają rozmieszczenie honeypotów.





Dużym wyzwaniem było umieszczenie honeypotów w tak wielu miejscach na świecie. Gdyby w każdym przypadku niezbędne było uzgodnienie umieszczenia sensora z jakimś podmiotem w danym kraju, mielibyśmy do czynienia z wielkim kosztem i wyzwaniem organizacyjnym. Trudno byłoby także skutecznie zdalnie administrować sensorami. Dlatego zdecydowano się na centralizację i standaryzację honeypotów.

Wszystkie honeypoty projektu działają w rzeczywistości w centrum systemu, na serwerach w jednym miejscu w Polsce. Funkcjonalność sondy jest natomiast bardzo prosta – musi ona jedynie przekierowywać całość ruchu przez tunel do centrum. Dzięki temu wymagania techniczne dla sond były niewielkie. Z łatwością mogły je spełnić nawet najtańsze komercyjne serwery wirtualne (VPS – Virtual Private Server), wynajmowane od około 50 dostawców na całym świecie. Miesięczny koszt takiego serwera to najczęściej od kilku do kilkunastu euro, choć w bardziej egzotycznych lokalizacjach usługi takie są znacznie droższe. Całość procesu konfiguracji i administracji sondy, przy założeniu że działa ona pod kontrolą odpowiedniej, popularnej i standardowej wersji systemu operacyjnego Linux, została zautomatyzowana. Dzięki temu manualne interwencje niezbędne są jedynie w szczególnych przypadkach.

W systemie wykorzystano 12 różnych typów honeypotów, emulujących wiele różnych usług, od powszechnych (WWW, poczta, SSH/Telnet, itp.) po bardziej specjalizowane (np. Weblogic, SCADA). Wszystkie zostały ustandaryzowane, tak aby mogły być automatycznie uruchamiane i połączone z sondami, i żeby mogły w tej samej formie przekazywać zarejestrowane przez siebie zdarzenia.

W ciągu roku sieć SISSDEN zarejestrowała blisko 1,8 miliarda zdarzeń, informując o nich zainteresowane podmioty.

Darknet – teleskop internetowy

Innym źródłem informacji o zagrożeniach wykorzystywanym przez SISSDEN jest darknet (używana jest też nazwa „teleskop internetowy"). Darknet to nieużywany, ale obserwowany zakres adresów IP. Nie ma w nim żadnych usług, do których mógłby być kierowany ruch. Dlatego jakiekolwiek skierowane tam pakiety są z zasady podejrzane. W przeciwieństwie do honeypotów, w darknecie nie są emulowane usługi, a to oznacza, że żaden z pakietów nie otrzymuje żadnej odpowiedzi. Pozwala to uzyskać skalowalność i obniża ryzyko rozpoznania jako sondy, a co za tym idzie: znalezienia się na czarnych listach przestępców, omijanych w przyszłych działaniach. W rezultacie znacznie ograniczona jest także ilość danych. Zwłaszcza w przypadku ruchu TCP zasadniczo należałoby się spodziewać jedynie prób otwarcia połączenia lub (w przypadku podmienionego adresu IP) odpowiedzi na nie, bez możliwości ustalenia, do czego to połączenie miałoby być wykorzystane. Z pozoru są to więc dane ubogie i mało użyteczne.

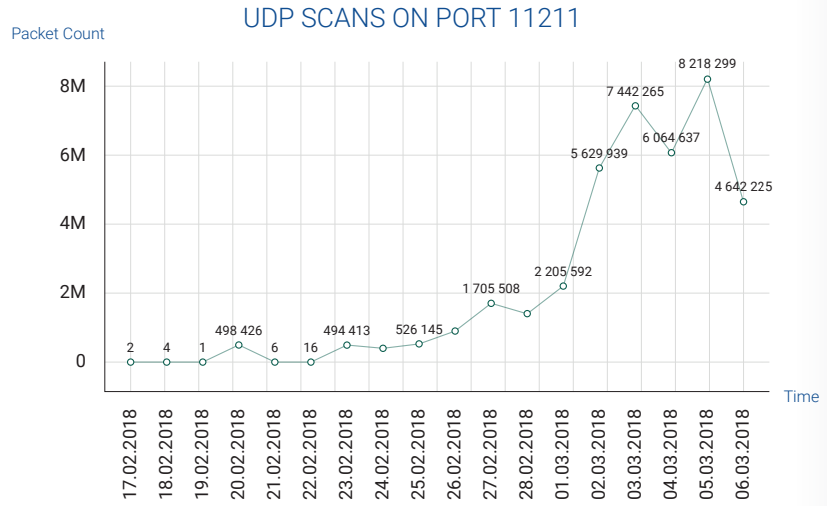
NASK dysponuje jednym z największych w rejonie darknetów, dlatego ilość pozyskiwanych danych jest bardzo duża. Dzięki opracowanym w projekcie SISSDEN heurystycznym analizom, dane te są bardzo użyteczne w praktyce. W darknecie widoczne są m.in. różnego rodzaju skanowania, a także odbicia ataków DDoS wykonywanych z podstawieniem losowych adresów IP. Szczególnie użyteczna analiza wykrywa w zarejestrowanych pakietach sygnatury różnych algorytmów generacji pakietów. Przy skanowaniach, a zwłaszcza przy atakach DDoS, zawartość pakietów wysyłanych przez botnety jest często generowana automatycznie przy użyciu bardzo uproszczonych algorytmów, w celu maksymalizacji wydajności. Pozostawia to charakterystyczne ślady, które mogą być automatycznie wykryte. Na przykład pojawienie się znacznego wzrostu ruchu na jakimś porcie niewiele mówi o jego pochodzeniu, ale jeśli w pakietach tych docelowy adres IP jest taki sam, jak numer sekwencji, można podejrzewać, że za działanie jest odpowiedzialny klon oprogramowania Mirai.

Ostrzeganie o zagrożeniach

Podstawowym celem zbierania danych jest **świadczenie bezpłatnej usługi informowania o zarejestrowanych zdarzeniach**. Informacje rozsyłane są w formie dobowych raportów do ponad czterech tysięcy odbiorców, z wykorzystaniem istniejących mechanizmów używanych przez Shadowserver.

Projekt SISSDEN zaowocował pięcioma nowymi typami raportów. Odbiorcy to głównie narodowe zespoły CERT w 80 krajach oraz właściciele poszczególnych sieci. Dostarczane informacje są filtrowane, dzięki czemu każdy odbiorca otrzymuje informacje tylko o tych zdarzeniach, które go dotyczą. Dostarczone informacje służą do identyfikacji zainfekowanych komputerów bądź nieuczciwych użytkowników. Jak wskazują wyniki sondy zrealizowanej w ramach projektu w kwietniu 2019 roku, użytkownicy oceniają otrzymywane informacje jako bardzo użyteczne przy rzeczywistym zwalczaniu zagrożeń.

Członkowie konsorcjum mają dostęp do funkcji analitycznych platformy, co również może mieć zastosowanie do zwalczania zagrożeń, chociażby przez działający w NASK zespół CERT Polska. Przykładem użyteczności dostępnych danych może być poniższy wykres, wykorzystujący dane z darknetu NASK.



Wykres dotyczy głośnej serii ataków DDoS z wykorzystaniem wzmocnienia poprzez publicznie dostępne serwery memcached, m. in. rekordowego ataku na Gitlab o intensywności 1,3 Tbit/s w dniu 28 lutego 2018 r. czy kolejnego rekordu – ataku z 5 marca 2019 r. o intensywności 1,7 Tbit/s.

Analiza rekordowego ataku na Gitlab

Memcached to sieciowa usługa pamięci podręcznej. Na udostępniającym ją serwerze można zapisać dowolną porcję danych z jakimś kluczem – w odpowiedzi na żądanie zawierające dany klucz, zawartość zostanie odesłana. Mechanizm ataku polegał na zapisaniu na takim serwerze (publicznym i niemającym uwierzytelniania, a więc zasadniczo wadliwie skonfigurowanym) dużej porcji danych, a następnie wysyłaniu do niego żądań z podszyciem się pod adres IP w celu ataku. W efekcie następowało potężne wzmocnienie – każdy pojedynczy pakiet mógł bowiem spowodować przesłanie do ofiary nawet megabajtów danych.

Przeprowadzenie takiego ataku wymaga wiedzy o wystarczającej liczbie takich niepoprawnie skonfigurowanych serwerów w Internecie. Wykres pokazuje, jak cenne może być bieżące śledzenie danych z darknetu. Port 11211, na którym działa memcached, jest mało popularny, toteż zazwyczaj rejestrowano na nim jedynie pojedyncze pakiety pochodzące z ogólnych skanów. Jednak 20 lutego 2019 r. nagle zarejestrowano ponad pół miliona skanowań. Trzy dni później skanowania powróciły, a ich intensywność już tylko rosła. A więc już ponad tydzień przed pierwszym wielkim atakiem, w darknecie widoczne było niespodziewanie duże zainteresowanie niepozornym portem.

To dość czasu, aby ustalić, do czego jest używany i zastanowić się nad tym, do czego może być wykorzystany. Dodatkowo jeśli uznamy, że nie mamy tu do czynienia z trudną do znalezienia podatnością programu, a po prostu złośliwym wykorzystaniem jego podstawowej funkcjonalności (która nie powinna być dostępna), możemy przewidzieć nadchodzące wydarzenia i uprzedzić zainteresowane podmioty. Takie działanie umożliwiłoby poprawną rekonfigurację usługi lub ustawienie filtrów ograniczających ruch przez właścicieli sieci. Dzięki temu możliwe byłoby znaczne ograniczenie skali ataków. Niestety jest to analiza historyczna. Darknet SISSDEN działał wówczas jeszcze w trybie testowym – dane były już zbierane, ale jeszcze niemonitorowane operacyjnie.

Analityka, sandboxy, śledzenie botnetów i inne

SISSDEN to także wiele innych źródeł i systemów. Wielka dostępna ilość danych umożliwia opracowywanie nowych metod analitycznych i wizualizacyjnych. Zadaniem tym zajmowało się wielu partnerów, a punktem styku była platforma analityczna realizowana przez Eclexys. Najciekawszą chyba analizą opracowaną w NASK jest mechanizm rozpoznawania dialektów SMTP, który wykorzystuje różnice w implementacji protokołu do identyfikacji oprogramowania rozsyłającego spam.

Próbki złośliwego oprogramowania zbierane przez honeypoty były poddawane analizie w systemach sandboksowych, czyli wirtualnych środowiskach do kontrolowanego uruchamiania programów. SISSDEN dysponował dwoma rodzajami sandboksów:

- **Krótkoterminowymi** – umożliwiały prostą analizę zachowania programu poprzez monitorowanie jego pracy przez zadany okres.
- **Długoterminowymi** – zapewniały możliwość śledzenia zmian zachowania wybranych próbek, które dysponowały mechanizmami zdalnego zarządzania i/lub aktualizacji. Takie próbki instalowane są na maszynie wirtualnej, która jest następnie uruchamiana wielokrotnie na przestrzeni wielu miesięcy, symulując rzeczywisty komputer domowy.

Rozwijane były także inne metody śledzenia botnetów. Na przykład w NASK rozwijano projekt mtracker, który umożliwia śledzenie różnych rodzin złośliwego oprogramowania poprzez emulację ich protokołów sterowania. Dzięki temu nowe konfiguracje oprogramowania (w tym cele i metody ataków) mogą być skutecznie rozpoznawane na bieżąco, bez ryzyka współuczestnictwa w atakach.

SISSDEN to także dane z innych źródeł należących zarówno do partnerów (np. T-Pot – system honeypotowy Deutsche Telekom,

czy AmpPot – honeypoty do wykrywania ataków wzmocnieniowych opracowane przez Universität des Saarlandes), jak i publicznie dostępnych. W efekcie w centrum systemu możliwa jest analiza i korelacja wielkich ilości wartościowych informacji, zapewniająca pełną świadomość sytuacyjną.

Co dalej?

Projekt SISSDEN zakończył się 30 kwietnia 2019 roku, osiągnąwszy swoje cele. Obecnie trwają prace związane z jego końcowym rozliczeniem. Techniki i narzędzia rozwinięte w projekcie są i będą nadal wykorzystywane przez partnerów w ich dalszej działalności. Produkty projektu wykorzystywane są szczególnie w NASK PIB – zarówno w pracach CERT Polska, jak i komercyjnego zespołu NIRT. Stanowią też zalążek i przedmiot dalszych prac w kolejnych uruchamianych w NASK projektach.

Jako że centrum systemu implementowane było na wynajętej infrastrukturze, po zakończeniu projektu zostało niestety wyłączone. Zebrane w czasie projektu dane zostały jednak zachowane i są udostępniane zainteresowanym oraz zweryfikowanym badaczom jako „Curated Reference Data Set". Komercyjni partnerzy konsorcjum przygotowują komercyjną wersję platformy z nowymi usługami. Sam system i oferowane przez niego publiczne usługi również zostaną niebawem przywrócone do działania. NASK i Shadowserver wyraziły gotowość dalszej współpracy, udało się już pozyskać częściowe finansowanie i ruszyły procedury zakupowe. Wkrótce można się spodziewać powrotu nieodpłatnych usług oferowanych przez platformę, tym razem realizowanych już na naszym własnym sprzęcie. Oznacza to, że raporty o zdarzeniach ponownie będą dostępne dla użytkowników.

Komentarz NASK

Komisja Europejska kładzie coraz większy nacisk na działalność badawczo – rozwojową. 12 września 2018 roku KE przedstawiła propozycję rozporządzenia ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych wraz z siecią krajowych ośrodków koordynacji. Jest to propozycja współpracy, której celem jest stymulowanie europejskiego ekosystemu technologicznego i przemysłowego w dziedzinie cyberbezpieczeństwa. Zgodnie z propozycją KE powstanie Europejskie Centrum Cyberbezpieczeństwa – nowa instytucja, której zasadniczą rolą ma być dystrybuowanie funduszy europejskich w dziedzinie cyberbezpieczeństwa z poziomu europejskiego na poziom państw członkowskich. Dodatkowo centrum ma gromadzić wiedzę i komptencje w zakresie cyberbezpieczeństwa. Poza Europejskim Centrum Cyberbezpieczeństwa powstanie sieć krajowych ośrodków koordynacji. Ośrodki te nominowane będą przez kraje członkowskie, a następnie akredytowane przez Komisję Europejską. Instytucje te mają wspierać działania centrum[63].

[63] *Więcej informacji na temat Rozporządzenia jest dostępnych na stronie https://cyberpolicy.nask.pl/europejskie-centrum-kompetencji-w-dziedzinie-cyberbezpieczenstwa-oraz-siec-krajowych-osrodkow-koordynacji-nowa-propozycja-ke/*

NASK
Cyber POLICY

Flash ze Stałego Przedstawicielstwa w Brukseli

Michał Czerniawski, Justyna Romanowska
Stałe Przedstawicielstwo RP w Brukseli

Czerwcowe posiedzenie Rady TTE

7 czerwca odbyło się posiedzenie Rady TTE. Na agendzie znalazły się m.in. debata strategiczna dotycząca przyszłości cyfrowej Europy po 2020 r. wraz z konkluzjami Rady „Zwiększenie cyfrowej i gospodarczej konkurencyjności i cyfrowej spójności w całej Unii", stanowisko UE na Światową Konferencję Radiokomunikacyjną (WRC 2019) oraz projekt rozporządzenia o e-prywatności.

W ramach punktów AOB pojawił się również **projekt Rozporządzenia w sprawie centrów doskonalenia cyberbezpieczeństwa** oraz Program Cyfrowa Europa.

Podczas publicznej debaty o przyszłości cyfryzacji ministrowie zwracali uwagę na rosnącą konkurencję globalną w obszarze nowych technologii nie tylko ze strony USA, ale także Chin. Dyskusja dotyczyła tego jak utrzymać konkurencyjność europejskich przedsiębiorców na globalnym rynku. Wskazywano na rosnącą rolę Sztucznej Inteligencji (AI), konieczność zapewnienia dostępu do dobrej jakości danych, zwłaszcza dla MŚP i startup'ów, rozwoju kompetencji cyfrowych, czy cyberbezpieczeństwa. Podkreślano także, że innowacyjność musi mieć miejsce przy poszanowaniu etyki oraz europejskiego systemu wartości. W dyskusji dotyczącej opodatkowania sektora cyfrowego, wszystkie p.cz. zgodziły się na przygotowany przez PREZ projekt konkluzji, odnoszący się do sprawiedliwego i uczciwego systemu, jednak kilka p.cz. podkreśliło, że kwestie podatkowe stanowią wyłączne kompetencje p.cz. i powinny być dyskutowane w ramach innych formacji Rady (Rada ECOFIN), a także na forum międzynarodowym (OECD).

W dyskusji dotyczącej projektu rozporządzenia o e-prywatności, dwa p.czł. podnosiły potrzebę wprowadzenia podstawy prawnej do walki z pornografią dziecięcą online, jedno p.czł. podkreśliło, że rozporządzenie nie powinno obniżać poziomu ochrony względem obecnie istniejącego, stąd nie może poprzeć tekstu, który proponowała PREZ RO, a jedno wskazało na niejasności pomiędzy tym projektem a RODO. Rada przyjęła raport z postępu prac nad tym projektem legislacyjnym.

W pozostałej niejawnej części posiedzenia przyjęto stanowisko UE na Światową Konferencję Radiokomunikacyjną (WRC 2019), PREZ RO omówiła aktywność Rady UE w obszarze otwierania danych publicznych (dyrektywa PSI) i cyberbezpieczeństwa, miała miejsce prezentacja 'Prague Proposals' dotyczących bezpieczeństwa sieci 5G oraz konieczności promowania bezpieczeństwa łańcucha dostaw oraz dobrych praktyk w obszarze cyberbezpieczeństwa, a także prezentacja planów PREZ FI.

Kolejna Rada TTE odbędzie się 3 grudnia 2019 r. w Brukseli.

NASK

Cyber POLICY

NASK Państwowy Instytut Badawczy
ul. Kolska 12, 01-045 Warszawa

ISBN 978-83-954637-0-9

cyberpolicy.nask.pl