

What's Up Wholesale?

Przegląd rynku operatorskiego 2025

zawiera badanie operatorów

**„Nowe wymogi regulacyjne i ich wpływ
na przedsiębiorstwa telekomunikacyjne
z sektora MŚP”**

Partner branżowy



Partner medialny



Wholesale

Spis treści

	Wstęp	3
1	Badanie	7
2	Prawo telekomunikacyjne	16
	Czas wyzwań regulacyjnych	17
	Problemy polskiego (mikro, małego, średniego) przedsiębiorcy telekomunikacyjnego	19
	Telekomy w nowym Krajowym Systemie Cyberbezpieczeństwa	24
	Telekomunikacja też podjęła rękawicę rzuconą przez premiera	27
	Od legislacyjnej teorii do rynkowej praktyki. Walka z CLI spoofingiem	29
	Chińskie Mury w pomarańczowym kolorze	31
3	Odporność sieci	33
	Odporność sieci: dezinformacja w telekomunikacji	34
	Odporność sieci: powódź	38
	Odporność sieci: klimat	41
	Odporność sieci: zagrożenia militarne	43
4	Okiem liderów rynku	48
	Infrastruktura w cenie	49
	Niezmiennie regulacje i zmieniający się rynek – perspektywy i wyzwania rynku hurtowego	53
	Rynek światłowodowy w Polsce dojrzał i wciąż ma przed sobą ogromny potencjał	55
	Rozwój Rynku Infrastruktury Telekomunikacyjnej: perspektywa Światłowodów Inwestycje	57
5	Technologie i komunikacja	60
	Trendy w sieciach optycznych i ich rola w ewolucji rynku	61
	Światłowodowe systemy czujnikowe – nowe możliwości i szanse dla operatorów sieci	70
	„Copper Switch Off” czyli wycofywanie z eksploatacji sieci miedzianych	73
	RCS-ie, czy „jesteś lekiem na całe zło”?	75
	Jak budować przewagę biznesową, gdy konkurencja ceną nie jest możliwa? Studium przypadku	81





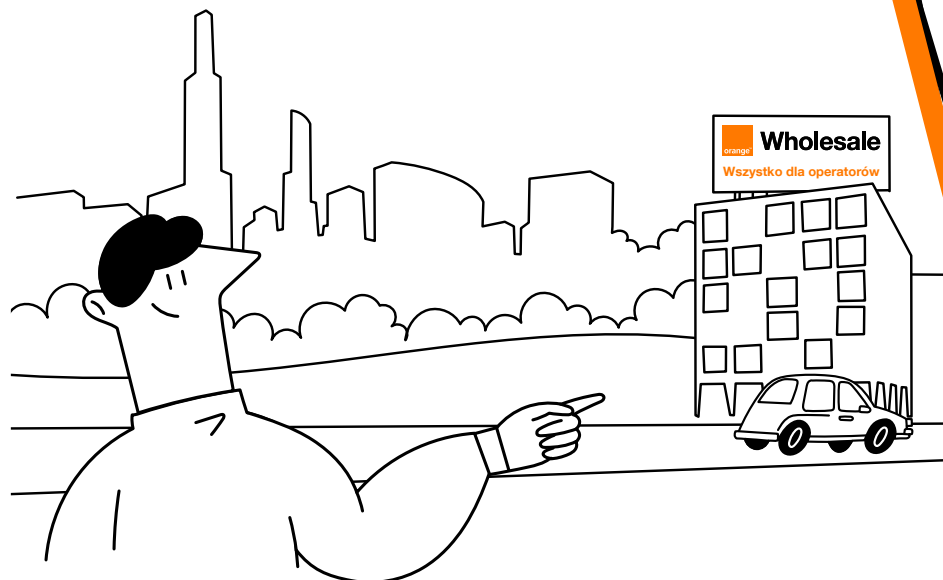
Milo mi zachęcić Was do lektury naszego najnowszego raportu o rynku operatorskim w Polsce. To już 5. raport z kolei, ale zapewniam, nie będziecie się nudzić. Znowu jest przepełniony wartościową treścią i nośnymi opiniami najlepszych ekspertów z branży. Dla mnie, moich koleżanek i kolegów z Orange bieżący czas jest szczególnie ważny. Właśnie zakończyliśmy realizację strategii „Grow i „odpaliliśmy” nową – Lead The Future, która wyznacza kierunki rozwoju w nadchodzących latach. Wierzymy, że współpraca z operatorami otworzy wszystkim nowe możliwości rozwoju i wzrostu.

To jaka jest nasza strategia?

Pandemia przyspieszyła rozwój rynku telekomunikacyjnego, zwiększając zapotrzebowanie na szybki internet i nowe sieci światłowodowe. W ciągu ostatnich 4 lat sześciokrotnie zwiększyła się liczba klientów hurtowych na naszej sieci FTTH, sprzedaliśmy ponad 2 razy więcej transmisji danych, prawie 1,5 raza więcej kanalizacji oraz czterokrotnie więcej słupów. Operatorzy, korzystając z naszej infrastruktury, mogli efektywnie rozwijać swoje sieci, wspierając się również funduszami unijnymi.

Prognozy wskazują jednak, że do 2028 roku cały kraj będzie miał dostęp do szybkiego internetu poprzez światłowód lub sieci 5G. Zmieni to dynamikę rynku, a kluczowe stanie się efektywne wykorzystanie istniejącej infrastruktury, szczególnie na obszarach o korzystnej strukturze demograficznej. Dla wielu operatorów szansą na rozwój będzie skorzystanie z dostępu hurtowego. Jako właściciel największej otwartej sieci planujemy – w ramach strategii Lead The Future – zwiększyć do 2028 roku bazę klientów hurtowych na światłowodzie o 50%. Dziś mamy 80 klientów-operatorów korzystających z usług BSA FTTH. W najbliższej przyszłości, to właśnie efektywne korzystanie z sieci innych podmiotów będzie receptą na wzrost.

Nasza nowa strategia opiera się na idei one-stop-shop, którą doskonale oddaje hasło „wszystko dla operatorów”. Chcemy być dla naszych partnerów punktem kompleksowej obsługi, oferując im zarówno nowoczesne rozwiązania, jak i wsparcie na każdym etapie współpracy. Zapewniamy im dostęp do kompletnego portfolio usług, które zaspokoi wszystkie ich potrzeby, w tym narzędzia do budowania konwergentnych ofert dla klientów końcowych, obejmujących również usługi MVNO. Stawiamy na profesjonalną obsługę, przejrzyste procesy i sieć budowaną według najwyższych standardów. To wszystko składa się na obraz Orange Polska jako rzetelnego i atrakcyjnego partnera dla każdego operatora, niezależnie od wielkości jego sieci.



Konsolidacja i współpraca międzyoperatorska

Od lat branża telekomunikacyjna jest pod dużą presją oczekiwanego zwrotu z kapitału, komodytyzacji usług telekomunikacyjnych i rosnących kosztów. W poszukiwaniu efektywności rynek konsoliduje się i jednocześnie kreuje nowe formy współpracy.

Najczęściej wskazywaną formą konsolidacji są wspólne przedsięwzięcia z innymi firmami (42%). Jednak znaczący odsetek respondentów (27%) otrzymał propozycje przejęcia przez dużych operatorów, a 19% przez inne małe i średnie przedsiębiorstwa.

42%

Wspólne przedsięwzięcia z innymi firmami

27%

Propozycje przejęcia przez dużych operatorów

19%

Propozycje przejęcia przez małych i średnich operatorów

W tej sytuacji coraz większe znaczenie ma otwartość operatorów na współdzielenie informacji o swojej infrastrukturze. Od kilku lat zapraszamy małych i średnich ISP do współpracy w ramach modelu rBSA lub aplikacji hurtowej Focus, która umożliwia prezentację infrastruktury lokalnych operatorów. Przekazane dane możemy wykorzystać zestawiając połączenia dla klientów-operatorów na rynku międzynarodowym i krajowym. Dzięki Focusowi osiągamy efekt „win-win-win” – nasi klienci zyskują tańsze połączenia, Orange optymalizuje wykorzystanie sieci, a właściciele infrastruktury generują dodatkowe przychody.

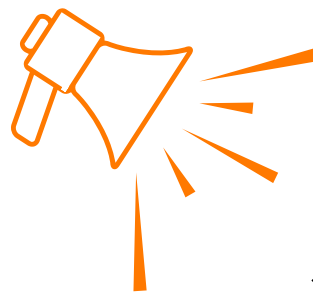
Jeszcze kilka lat temu trudno było sobie wyobrazić, że współpraca między operatorami na taką skalę będzie możliwa. Dziś obserwujemy rosnące zainteresowanie tym modelem, co potwierdza liczba operatorów chcących dołączyć do platformy Focus. Do współpracy zgłosiło się już blisko 20 firm. Zamierzamy intensywnie rozwijać platformę, ponieważ wierzymy, że współpraca to klucz do sukcesu na dynamicznie zmieniającym się rynku telekomunikacyjnym. Nasza strategia "wszystko dla operatorów" to zobowiązanie do budowania partnerskich relacji i dostarczania rozwiązań, które pomogą w rozwoju biznesu.



Zmieniamy się

W 2024 roku kontynuowaliśmy rozwój naszej oferty. Oprócz nowych zasięgów na światłowodzie hurtowym, wdrożyliśmy nowe funkcjonalności w naszych usługach. Operatorzy MVNO zyskali możliwość korzystania z roamingu w wybranych krajach, a w Strefie Operatora (dawniej POKO) udostępniliśmy nowy moduł do zarządzania umowami dla Kanalizacji Kablowej i Słupów.

Rozwijamy również nasze kanały cyfrowe, aby współpraca była jeszcze łatwiejsza i bardziej efektywna. W efekcie odnotowaliśmy niemal dwukrotny wzrost udziału zamówień online na usługi infrastrukturalne. Automatyzacja procesów technicznych, takich jak wywiady techniczne, pozwoliła zwiększyć ich udział o 10%. Zoptymalizowaliśmy również proces obsługi zgłoszeń awarii Transmisji Danych, skracając czas reakcji. Dodatkowo udostępniliśmy bardziej precyzyjne mapy cyfrowe, nową stronę internetową dla użytkowników TPIX oraz zwiększyliśmy do 80% udział faktur elektronicznych.



Wdrożyliśmy

- **MVNO**: możliwość uruchomienia roamingu w wybranych krajach
- **Nową stronę internetową** dla TPIX



Udostępniliśmy

- **2,5 mln** zasięgów na najkorzystniejszych warunkach na rynku
- **Nowy moduł** zarządzania Umowami dla Kanalizacji kablowej i Słupów w POKO



Zwiększyliśmy

- do **97%** usług infrastrukturalnych zamawianych cyfrowo
- o **10%** udział automatycznych Wywiadów Technicznych i jakość danych na mapach w POKO



Skróciliśmy

- o **10%** czas reakcji na zgłoszone uszkodzenia DATA (POKO)



Jesteśmy EKO

- do **80%** zwiększyliśmy udział e-faktur



OJ, POZMIENIAŁO SIĘ W TYM 2024!

Branża o deregulacji

W tegorocznym badaniu zapytaliśmy blisko 200 małych i średnich operatorów o ich opinie na temat toczących się procesów legislacyjnych. W dobie wprowadzania licznych nowych przepisów operatorzy oczekują uproszczeń i zmian, które realnie ułatwią prowadzenie działalności.

Choć respondenci doceniają coraz większe otwarcie strony publicznej na konsultacje z branżą, to wskazują, że w niektórych przypadkach z trudem dostrzegają celowość wprowadzanych regulacji. Mają też trudności z ich interpretacją. Mierząc się z wysokimi kosztami dostosowywania do nowych wymogów, liczą, że obietnica odwilży regulacyjnej i podjęte prace nad uproszczeniem wymogów prawnych pomogą usunąć dotychczasowe przeszkody. Operatorzy oczekują przede wszystkim ułatwień i zniesienia barier inwestycyjnych związanych z rozbudową sieci, takich jak zajęcie pasów drogowych czy uproszczenie procedur budowlanych. Istotne jest także ułatwienie dostępu do terenów kolejowych, dróg wewnętrznych oraz infrastruktury obcej, w tym energetycznej.

Czytelnik 5. edycji raportu znajdzie w nim wiele praktycznych wskazówek z zakresu wprowadzanych w prawie zmian. O opinię poprosiliśmy m.in. przedstawicieli izb gospodarczych, angażujących się na co dzień w prace z Regulatorem. Szczególne podziękowania składam na ręce Andrzeja Dulki, prezesa PIIT, Joanny Sikory – Koordynatora Międzyizbowego Zespołu Telekomunikacyjnego ds. Deregulacji, prezesa ZTKiG Pawła Wołocha oraz KIKE, która objęła ponownie patronatem nasz raport. Nie brakuje też głosów z branży – hurtowników (Światłowód Inwestycje, Nexera i Fiberhost) oraz firm technologicznych, takich jak Nokia. Wszystkim partnerom merytorycznym dziękujemy, a czytelników zapraszamy do lektury.



1 Badanie

Nowe wymogi regulacyjne i ich wpływ na przedsiębiorstwa telekomunikacyjne z sektora MŚP

Badanie przeprowadziliśmy w lutym 2025 roku za pomocą kwestionariuszy online. Celem było zebranie opinii operatorów o wpływie wybranych zmian regulacyjnych na ich działalność biznesową, w tym m.in.: PKE, KSC, SCP, KSeF.

W ankiecie udział wzięło 192 respondentów – głównie przedstawiciele segmentu małych i średnich ISP.

Wyniki ankiety oraz ich omówienie nie stanowią opinii Orange Polska S.A.



Omówienie badania

Prawo Komunikacji Elektronicznej

Wprowadzenie Prawa Komunikacji Elektronicznej (PKE) było jednym z najważniejszych wydarzeń w branży. PKE zastąpiło ustawę Prawo Telekomunikacyjne, która obowiązywała przez ostatnie 20 lat. Nowe regulacje miały na celu dostosowanie polskiego rynku do dynamicznie zmieniających się realiów technologicznych i prawnych.

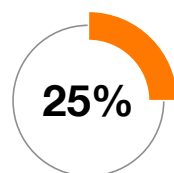
Jednak, jak pokazują wyniki badania, wdrożenie PKE okazało się dla wielu przedsiębiorców wyzwaniem, które wymagało nie tylko czasu i zasobów, ale także dużego zaangażowania pracowników. Co trzeci ankietowany uznał nowe prawo za rewolucję.

Co ułatwiło wdrożenie PKE?

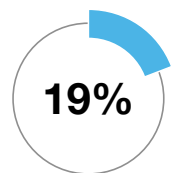
Wśród czynników, które ułatwiły wdrożenie Prawa Komunikacji Elektronicznej, najczęściej (25%) wskazywano fakt, że w procesie legislacyjnym uwzględniono stanowiska izb gospodarczych reprezentujących małych i średnich operatorów. 44% respondentów wskazało, że najaktywniej interesy małych i średnich operatorów reprezentowała KIKE. Kolejnym ważnym czynnikiem były długie konsultacje ustawy z branżą (19%), które pozwoliły przedsiębiorcom lepiej przygotować się do zmian oraz jasne sformułowanie treści ustawy docenione przez 17% ankietowanych.

W odpowiedziach otwartych często pojawiały się wskazania na pomoc kancelarii prawnych oraz szkolenia.

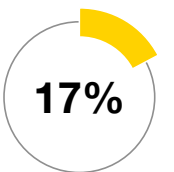
Co w największym stopniu ułatwiło Ci wdrożenie PKE?
(wybór wielokrotny)



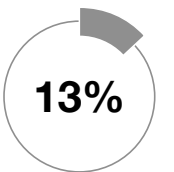
Uwzględnienie stanowisk izb gospodarczych reprezentujących małych i średnich operatorów



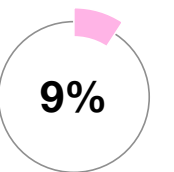
Długie konsultacje ustawy z branżą



Jasne sformułowanie treści ustawy



Jaka inna rzecz w największym stopniu ułatwiła Ci wdrożenie PKE?



Wsparcie informacyjne od Ministerstwa Cyfryzacji

Omówienie badania

Co utrudniło wdrożenie PKE?

Największym problemem okazał się krótki czas na wdrożenie, na który wskazał co trzeci respondent. Kłopotliwy był także termin wdrożenia wyznaczony na ostatnie miesiące roku (21%).

Kolejnym istotnym problemem były niejasne zapisy treści ustawy (19%), które wymagały interpretacji i dodatkowego wsparcia prawnego. W odpowiedziach otwartych pojawiały się głosy krytyczne, wskazujące na brak realnych konsultacji z mniejszymi operatorami oraz nadmierne regulacje, które zdaniem niektórych respondentów nie wnoszą wartości dodanej.

Co w największym stopniu utrudniło Ci wdrożenie PKE?

(wybór wielokrotny)

29%

Krótki czas na wdrożenie

21%

Termin wdrożenia wyznaczony na ostatnie miesiące roku

19%

Niejasne zapisy treści ustawy

Z czego korzystała Twoja firma, aby wdrożyć PKE?

(wybór wielokrotny)

43%

Usług kancelarii prawnych

15%

Opracowań przygotowanych przez izby gospodarcze

15%

Usług informatycznych firm zewnętrznych

14%

Żadnych z powyższych

13%

Szkoleń dla pracowników

Wsparcie prawne kluczem do sukcesu

Wdrożenie PKE wymagało od przedsiębiorców skorzystania z różnych form wsparcia. Najczęściej wybieranym rozwiązaniem były usługi kancelarii prawnych, na które wskazało aż 43% respondentów.

To pokazuje, że interpretacja nowych przepisów była na tyle skomplikowana, że firmy musiały polegać na specjalistach. Warto zauważyć, że opracowania przygotowane przez izby gospodarcze (15%) i szkolenia dla zespołów (13%) odegrały mniejszą rolę.

Koszty wdrożenia to nawet kilkadziesiąt tysięcy złotych

Jednym z kluczowych aspektów są koszty wdrożenia PKE. Co piąta firma przeznaczyła na dostosowanie się do nowych przepisów środki przekraczające 20 tys. zł. Wydatki rosły wraz z wielkością firmy. Na najwyższe obciążenia wskazała ponad połowa firm posiadających 5 tys. i więcej klientów, podczas gdy w przypadku mniejszych operatorów było to nieco ponad 40%.

To znaczące obciążenie dla przedsiębiorców telekomunikacyjnych, którzy często musieli korzystać z odpłatnych usług prawnych i informatycznych. Warto zauważyć, że koszty te nie ograniczały się jedynie do jednorazowych wydatków – wiele firm musiało zainwestować w dodatkowe zasoby.



Omówienie badania

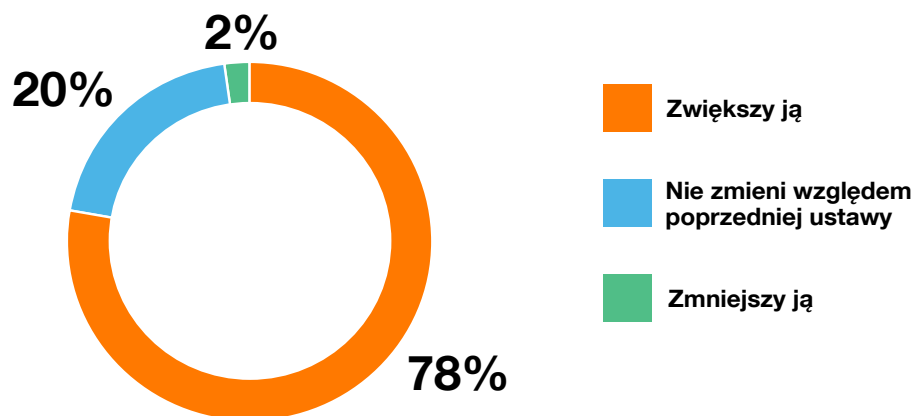
Pracownicy na pierwszej linii

Wdrożenie PKE miało istotny wpływ na pracowników firm telekomunikacyjnych. Aż 77% respondentów wskazało, że proces ten znacząco obciążył ich zespoły, a w 15% firm we wdrażanie nowych regulacji zaangażowana była ponad połowa personelu. W wielu przypadkach dodatkowa praca miała wpływ na bieżące funkcjonowanie firm.

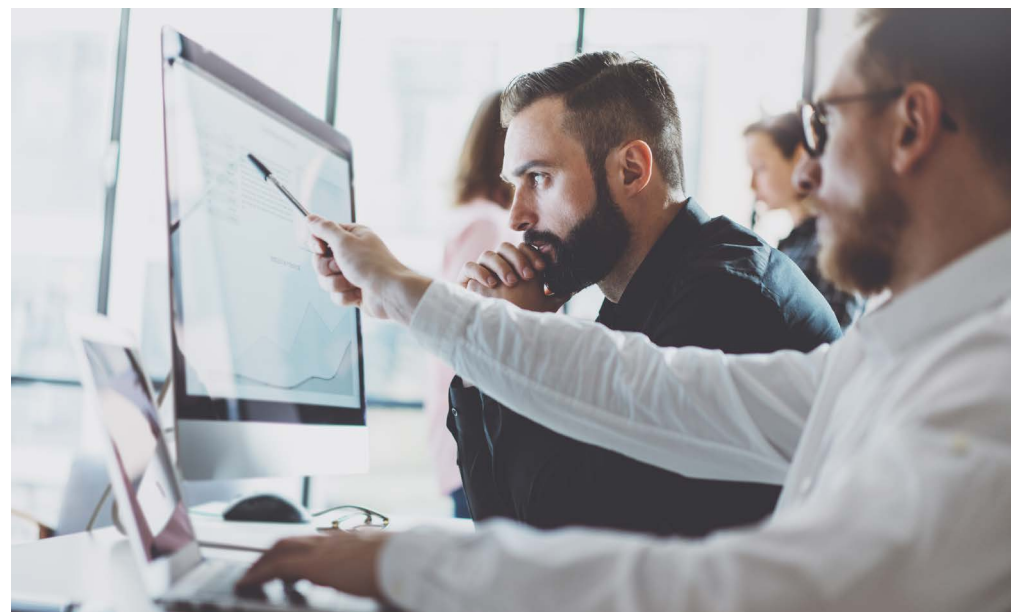
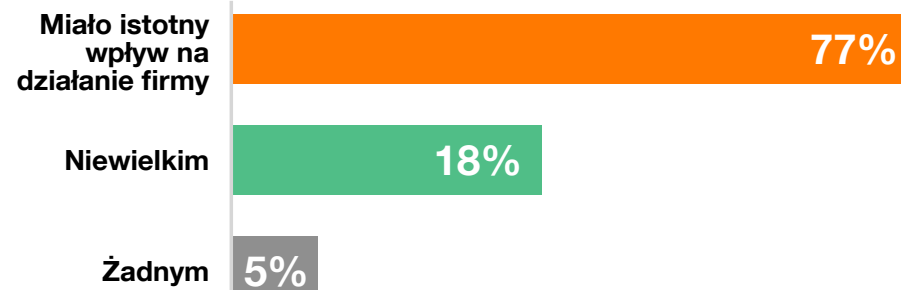
Pracochłonność wzrośnie – co dalej?

78% respondentów uważa, że realizacja obowiązków wynikających z PKE zwiększy pracochłonność w ich firmach. Tylko 2% przedsiębiorców spodziewa się zmniejszenia nakładu pracy. Szczególnie mniejsze podmioty, które obsługują mniej niż 5 tys. klientów i dysponują ograniczonymi zasobami obawiają się dodatkowych obciążeń. 36% z nich uważa, że będą one bardzo znaczące. W przypadku większych firm taką obawę wyraża co czwarty przedsiębiorca.

W jakim stopniu realizacja obowiązków z PKE wpłynie na pracochłonność w Twojej firmie?



W jakim stopniu wdrożenie PKE obciążyło pracowników Twojej firmy dodatkową pracą?



Krajowy System Cyberbezpieczeństwa

Projekt nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa przewiduje wprowadzenie pojęcia dostawcy wysokiego ryzyka (DWR). Firmy telekomunikacyjne o obrotach powyżej 10 mln zł lub świadczące usługi o krytycznym znaczeniu dla danego sektora będą musiały usunąć produkty wskazanych dostawców ze swoich sieci.



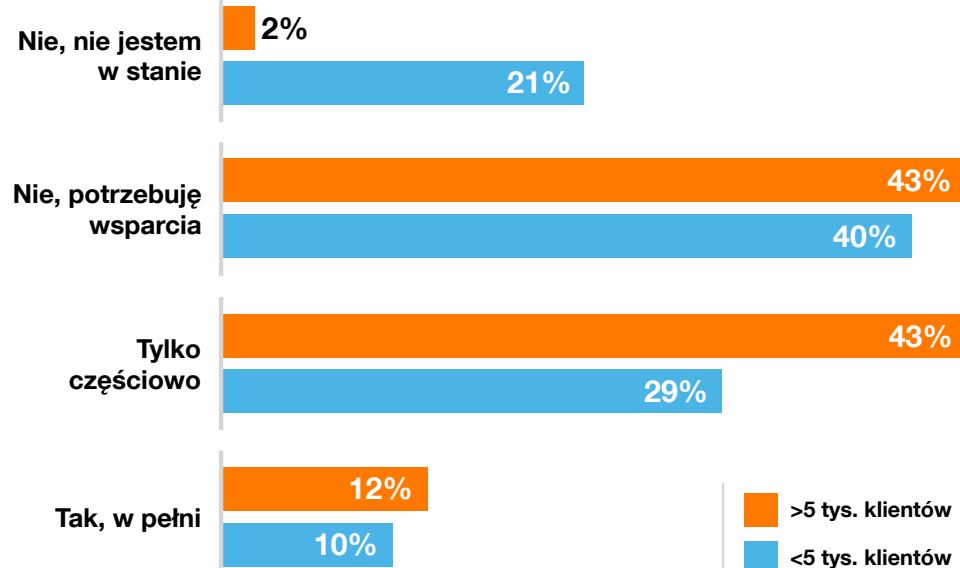
Dostępność zasobów do usunięcia produktów DWR

90% ankietowanych zadeklarowało, że nie będzie w stanie samodzielnie wdrożyć nowej regulacji. Większość z nich (40%) wskazuje, że potrzebowałoby wsparcia, aby sprostać obowiązkowi DWR. Ponad jedna trzecia posiada zasoby częściowo. Tylko co dziesiąty deklaruje pełną gotowość.

W komentarzach operatorzy podkreślają m.in. brak dostępnego sprzętu od alternatywnych dostawców oraz wysokie koszty wymiany. Wskazują również na problemy z kompatybilnością nowego sprzętu z istniejącą infrastrukturą oraz konieczność integracji z systemami, co generuje dodatkowe koszty i trudności organizacyjne.

Większe firmy (powyżej 5 tys. klientów) częściej deklarują, że posiadają zasoby do usunięcia sprzętu DWR ze swojej infrastruktury.

Czy posiadasz wystarczające zasoby, aby usunąć produkty DWR ze swojej sieci?



Krajowy System e-Faktur

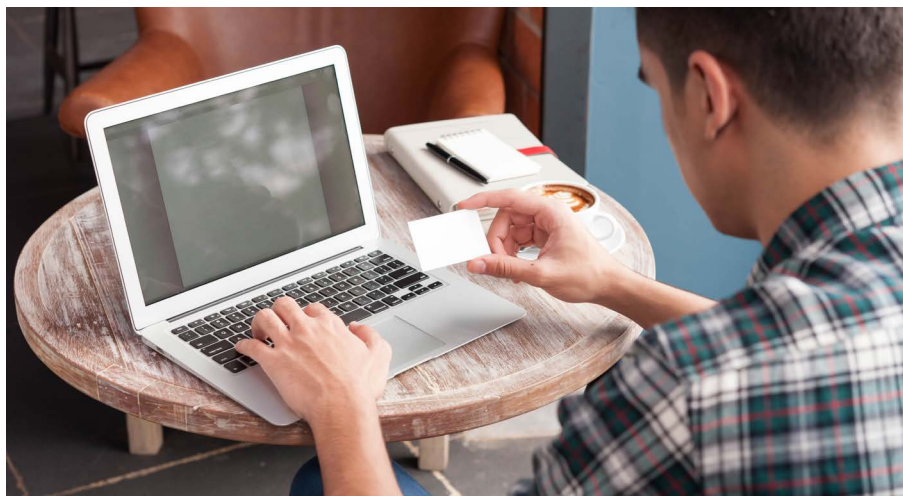
KSeF to system do wystawiania i otrzymywania faktur elektronicznych. Jest wdrażany przez Ministerstwo Finansów. Będzie obowiązkowy od 2026 roku dla większości firm.

Obawy przedsiębiorców

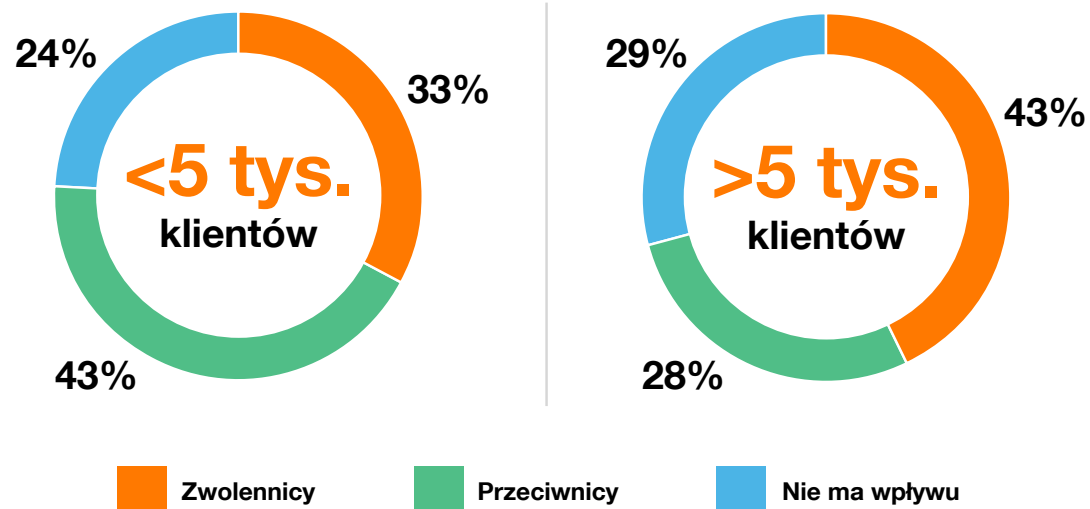
Już co trzeci ankietowany postrzega KSeF jako ułatwienie prowadzonej działalności. Podobna liczba uważa jednak, że utrudni on prowadzenie biznesu. Przedstawiciele większych firm częściej dostrzegają korzyści, podczas gdy respondenci z mniejszych są bardziej sceptyczni.

Problemy techniczne i koszty wdrożenia

Przedsiębiorcy obawiają się awarii i niskiej wydajności KSeF, szczególnie w kluczowych momentach, takich jak początek miesiąca. Wskazują na wcześniejsze problemy z systemami rządowymi, jak ePUAP czy JPK. Dodatkowo martwią się wysokimi kosztami dostosowania oprogramowania oraz wydatkami na aktualizacje wynikające ze zmieniających się przepisów.



Wpływ KSeF



Dostosowanie systemów i brak jasnych wytycznych

Integracja KSeF z obecnymi systemami informatycznymi wymaga czasu, zasobów i odpowiedniej infrastruktury, co jest wyzwaniem dla mniejszych firm. Przedsiębiorcy wskazują też na brak jasnych wytycznych dotyczących wdrożenia oraz obawy przed ciągłymi zmianami w przepisach.

Bezpieczeństwo danych i wpływ na działalność

Obawy dotyczą też ryzyka wycieków danych i nadmiernej kontroli fiskalnej. Respondenci w komentarzach podkreślają, że odpowiedzialność za błędy systemu spoczywa na nich, mimo że nie mają wpływu na jego działanie. Dodatkowo wdrożenie KSeF może zwiększyć obciążenia administracyjne i odciągnąć uwagę przedsiębiorców od kluczowych działań biznesowych.

Strategia Cyfryzacji Polski

Pod koniec ubiegłego roku Minister Cyfryzacji przedstawił Strategię Cyfryzacji Polski do 2035 roku. Jej celem jest poprawa życia obywateli dzięki cyfrowej transformacji państwa i firm. Część planów zależy od firm telekomunikacyjnych i wpłynie na przyszłe przepisy.

Niska świadomość SCP wśród przedsiębiorców

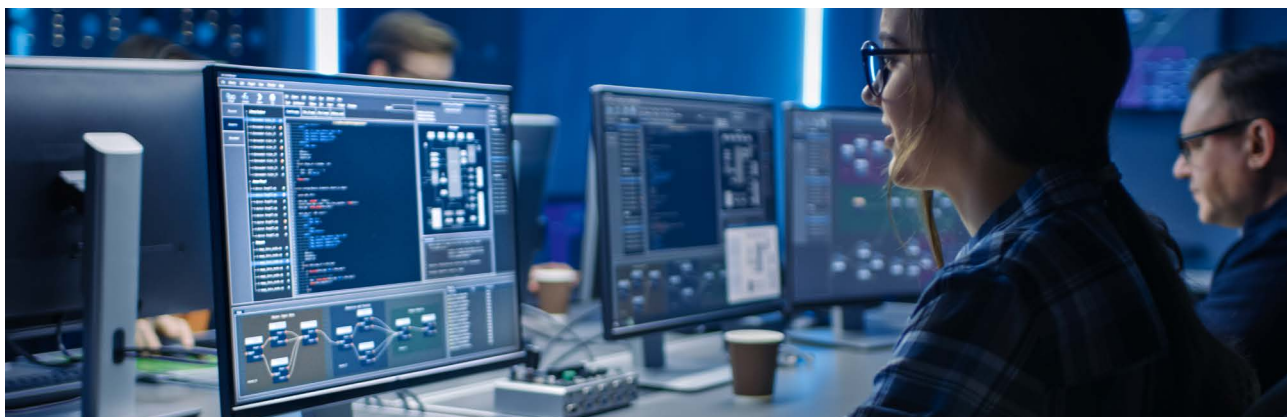
Mniej niż połowa ankietowanych (43%) słyszała o SCP, a zaledwie co piąty respondent zapoznał się z jej zapisami. Tylko 12%, z tych którzy ją znają wierzy, że realizacja strategii pozwoli osiągnąć zakładane cele, takie jak poprawa jakości życia obywateli czy wzrost konkurencyjności gospodarki. Jednocześnie blisko 70% nie ma zdania na ten temat, co może wynikać z braku wystarczających informacji.

Finansowanie inwestycji w białych plamach

W kwestii finansowania inwestycji w tzw. białych plamach, połowa respondentów popiera wykorzystanie środków publicznych, a jedna czwarta jest temu przeciwna.

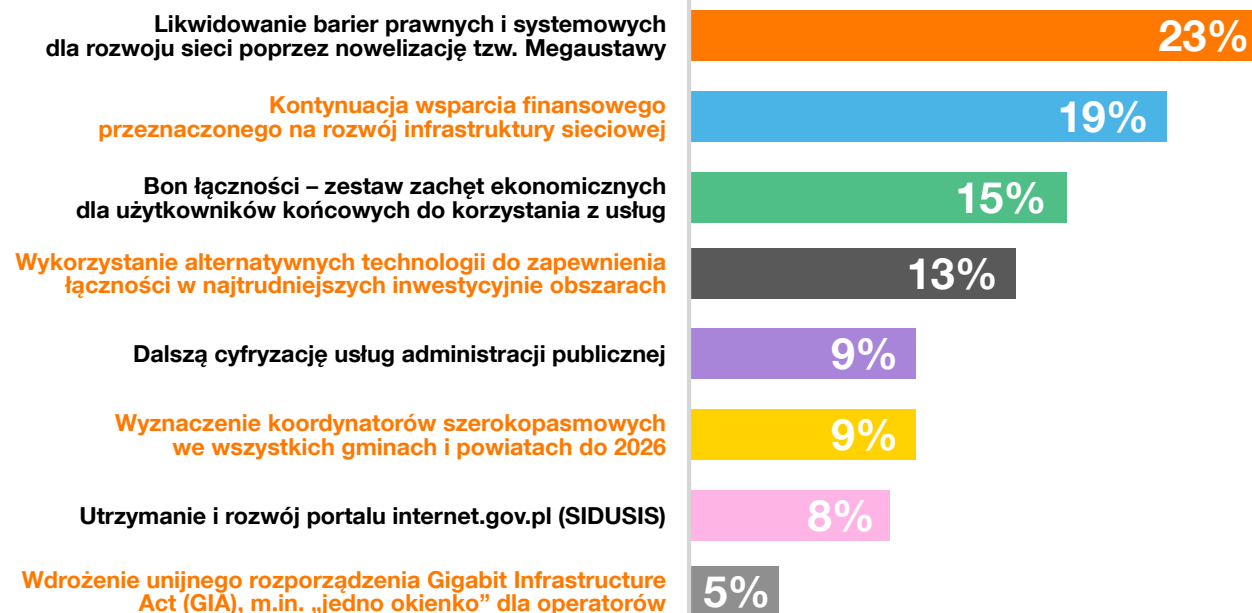
Priorytety działań w ramach SCP 2035

Wśród działań priorytetowych największe poparcie uzyskały likwidowanie barier prawnych i systemowych oraz kontynuacja wsparcia finansowego na rozwój infrastruktury sieciowej. Mniejsze zainteresowanie wzbudziły takie inicjatywy jak wdrożenie unijnego rozporządzenia Gigabit Infrastructure Act, czy rozwój portalu internet.gov.pl.



Które z poniższych działań z SCP 2035 ułatwi małym i średnim operatorom udział w transformacji cyfrowej społeczeństwa?

(wybór wielokrotny)



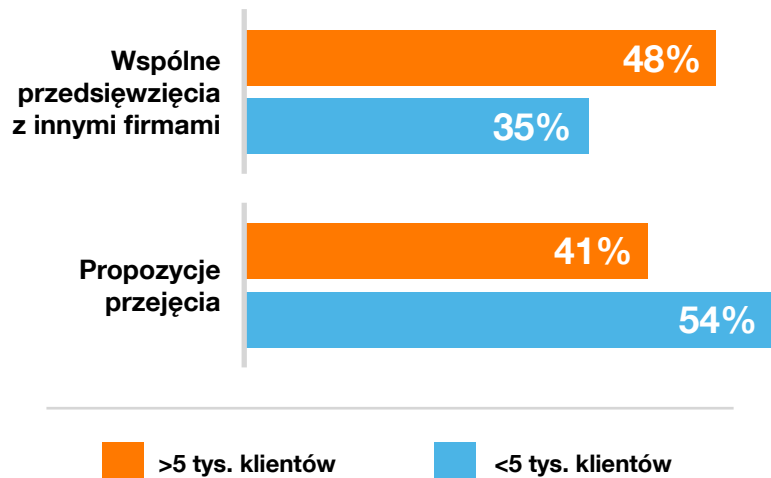
Konsolidacja

Operatorzy zauważają rozwijający się trend współpracy hurtowej oraz konsolidacyjny. 64% respondentów potwierdziło nasilenie tego zjawiska w różnych formach – od wspólnych przedsięwzięć po propozycje przejęcia.

Formy współpracy – wspólne działania i przejęcia

Najczęściej wskazywaną formą konsolidacji są wspólne przedsięwzięcia z innymi firmami (42%). Jednak znaczący odsetek respondentów (27%) otrzymał propozycje przejęcia przez dużych operatorów, a 19% przez inne małe i średnie przedsiębiorstwa. Zjawisko to wskazuje na dynamiczne zmiany w strukturze rynku. Ocena w pewnym stopniu zależy jednak od wielkości firmy. Przedsiębiorcy obsługujący poniżej 5 tys. klientów w większym stopniu spotykają się z propozycją przejęć niż wspólnych przedsięwzięć. Tym niemniej propozycję kooperacji otrzymało 35% małych operatorów i blisko połowa większych, co wskazuje na duży rozwój współpracy na rynku hurtowym.

Jakich zmian dotyczy odczuwana przez Ciebie presja konsolidacyjna?



Jakich zmian w prawie najbardziej potrzebują przedsiębiorcy w 2025 roku?

Na zakończenie badania zapytaliśmy respondentów o ich priorytety dotyczące nowych legislacji, które byłyby najbardziej potrzebne w bieżącym roku. Wyniki jasno pokazują, że przedsiębiorcy telekomunikacyjni oczekują przede wszystkim ułatwień w zakresie inwestycji i dostępu do infrastruktury.



Priorytety branży



Ułatwienia w procesie budowlanym

Najważniejsze są zmiany, które znoszą bariery inwestycyjne, takie jak zajęcie pasów drogowych czy uproszczenie procedur budowlanych. To wskazuje na potrzebę przyspieszenia i optymalizacji procesów związanych z rozbudową infrastruktury telekomunikacyjnej.



Ułatwienia w dostępie do nieruchomości

Drugim postulatem są zmiany umożliwiające łatwiejszy dostęp do terenów kolejowych, dróg wewnętrznych czy budynków. Przedsiębiorcy wskazują, że obecne regulacje często utrudniają rozwój sieci, co spowalnia procesy inwestycyjne.



Ułatwienia w dostępie do infrastruktury obcej

Dostęp do infrastruktury energetyki czy innych zasobów obcych również znalazł się wysoko na liście priorytetów. Wskazuje to na potrzebę lepszej współpracy międzysektorowej, która mogłaby przyspieszyć rozwój sieci telekomunikacyjnych.



Refinansowanie wydatków na wymianę sprzętu zgodnie z uKSC

W kontekście rosnących wymagań dotyczących bezpieczeństwa i zgodności z międzynarodowymi standardami, przedsiębiorcy oczekują wsparcia finansowego na wymianę sprzętu. To szczególnie istotne dla mniejszych firm, które mogą mieć trudności z pokryciem takich kosztów.



Łatwiejszy dostęp do produktów finansowych

Na końcu listy znalazły się postulaty dotyczące łatwiejszego dostępu do pożyczek i gwarancji finansowych. Choć mniej istotne niż kwestie infrastrukturalne, potrzeby finansowe wciąż pozostają ważnym elementem wspierającym rozwój branży.

2 Prawo telekomunikacyjne

- Krajowy System Cyberbezpieczeństwa
- Chińskie mury
- Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej
- Inicjatywa deregulacyjna „SprawdzaMy”



Czas wyzwań regulacyjnych



Andrzej Dulka
Prezes Zarządu
Polska Izba
Informatyki
i Telekomunikacji

Raport Orange Polska dotyczący rynku operatorskiego w 2025 roku pokazuje jasno, że aktualnie branża telekomunikacyjna w Polsce stoi przed szeregiem wyzwań regulacyjnych i technologicznych.

Uchwalenie Prawa Komunikacji Elektronicznej (PKE) stanowiło istotny krok w dostosowywaniu polskiego rynku do współczesnych realiów, jednakże wyniki badania wskazują, że proces ten był dla wielu przedsiębiorców trudny i kosztowny. Aż 33% respondentów określiło nowe przepisy jako rewolucję, a 77% badanych przyznało, że wdrożenie PKE znacząco obciążało ich zespoły. To bardzo ważny sygnał płynący wprost z rynku. Dodatkowo 78% firm uważa, że realizacja nowych obowiązków zwiększy pracochłonność w ich organizacjach. Kluczowym wyzwaniem okazał się krótki czas na wdrożenie, na który wskazał co trzeci respondent. Nowe regulacje związane z Krajowym Systemem Cyberbezpieczeństwa (KSC) będą również wyzwaniem i budzą obawy o ich skuteczność i wpływ na konkurencyjność branży.

Realne problemy, z którymi mierzą się dziś przedsiębiorcy mogą wpłynąć znacząco na konkurencyjność firm na rynku, ale także na ich rozwój, który przez liczne wymogi regulacyjne straci na dynamice. Te lokalne wyzwania wpisują się jednak w szerszy kontekst europejski, o czym świadczą m.in. niedawno opublikowane raporty Enrico Letty, Mario Draghiego oraz Sauli Niinistö. W publikacji „The future of European competitiveness” Draghiego podkreślono, że Europa musi zwiększać inwestycje w technologie cyfrowe, aby nadążyć za USA i Chinami. To bezpośrednio dotyczy polskiego rynku telekomunikacyjnego, który – jak pokazuje raport Orange – nadal zmagają się z regulacyjnymi barierami i koniecznością dostosowania infrastruktury. W tym kontekście ułatwienia legislacyjne dla przedsiębiorców, o które także zabiega PIIT, stanowią kluczowy element wzmacniania naszej pozycji na europejskiej mapie innowacji.

Z kolei raport Niinistö „Safer Together: Strengthening Europe’s Civilian and Military Preparedness and Readiness” zwraca uwagę na konieczność zabezpieczenia infrastruktury krytycznej, w tym telekomunikacyjnej, przed nowymi zagrożeniami. Jak wskazuje raport, w tej kwestii polskie firmy telekomunikacyjne obawiają się nadmiernych kosztów i skomplikowanych procedur związanych np. z wymianą sprzętu.



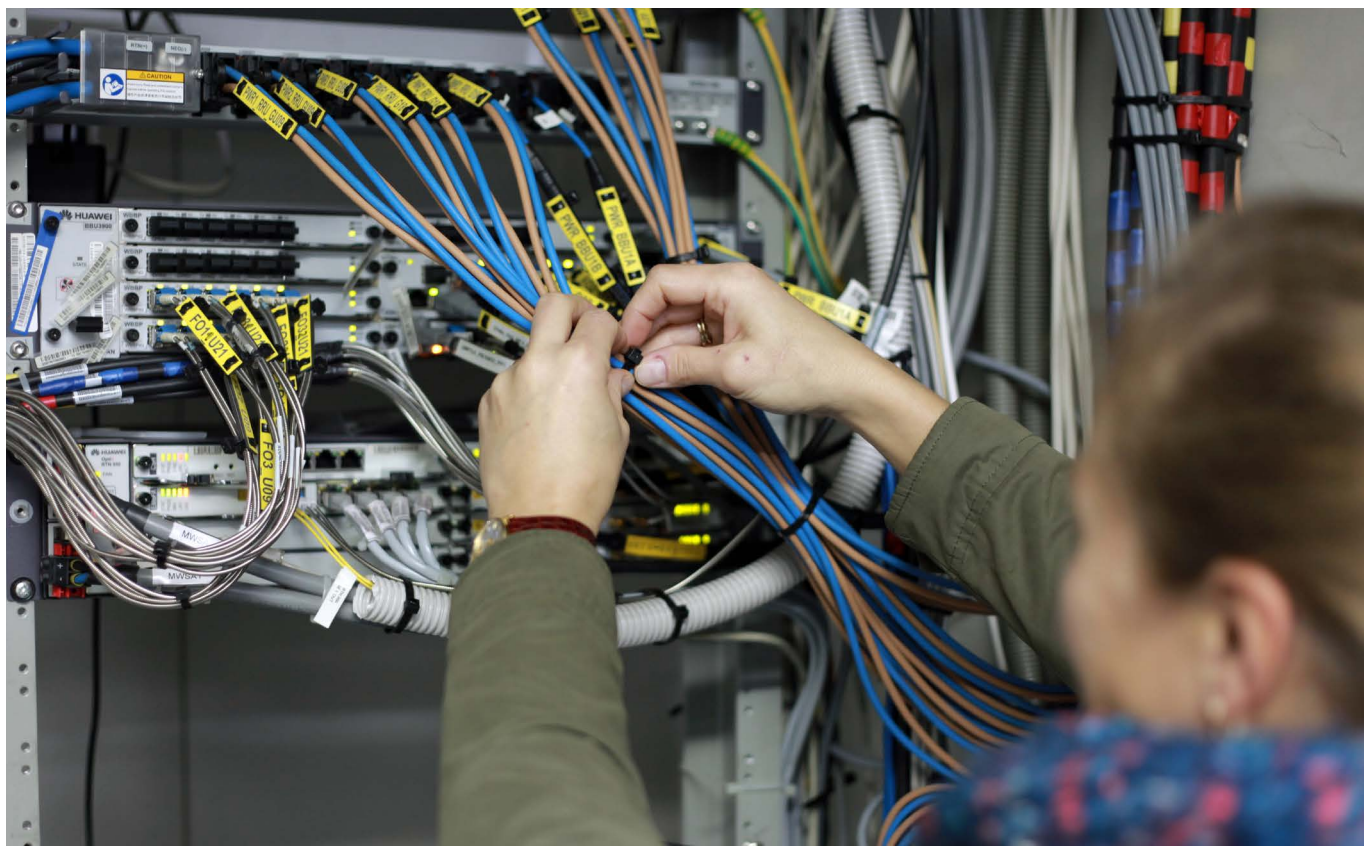
W dynamicznie zmieniającym się otoczeniu regulacyjnym kluczową rolę odgrywają inicjatywy dążące do ich uproszczenia. W Polsce operatorzy telekomunikacyjni mierzą się z licznymi barierami administracyjnymi, które utrudniają zarówno rozwój infrastruktury, jak i skuteczne funkcjonowanie na rynku. W odpowiedzi na te wyzwania eksperci Polskiej Izby Informatyki i Telekomunikacji aktywnie uczestniczą w pracach zespołu deregulacyjnego powołanego przez Premiera Donalda Tuska i koordynowanego przez Rafała Brzuskę, który skupia się na uproszczeniu przepisów i eliminowaniu barier dla przedsiębiorców. Priorytetem działań izby jest więc stworzenie środowiska, które nie tylko umożliwi operatorom sprawne funkcjonowanie w nowych realiach prawnych, ale także pozwoli im konkurować na arenie międzynarodowej.

PIIT jest przekonana, że dzięki wspólnemu zaangażowaniu sektora publicznego i prywatnego Polska ma szansę stać się liderem cyfryzacji w Europie, oferując obywatelom i przedsiębiorstwom nowoczesne, szybkie i stabilne usługi telekomunikacyjne. Dlatego też wraz z innymi izbami zgłosiliśmy inicjatywę powołania Zespołu ds. Rozwoju Telekomunikacji przy Ministerstwie Cyfryzacji.

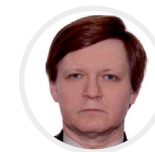
Jednym z kluczowych obszarów prac Zespołu będą kwestie związane z rozwojem infrastruktury telekomunikacyjnej, w tym identyfikacja barier legislacyjnych i administracyjnych ograniczających inwestycje oraz określenie sposobów ich eliminacji oraz kwestie finansowania realizacji strategicznych inwestycji.

Budowa infrastruktury cyfrowej to inwestycja w przyszłość Polski – zapewniająca gospodarczy wzrost, poprawiająca jakość życia obywateli i wzmacniająca konkurencyjność naszego kraju na arenie międzynarodowej. Polski sektor telekomunikacyjny ma ogromny potencjał, by stać się motorem cyfrowej transformacji. Jednak aby to osiągnąć, konieczne jest stworzenie bardziej przyjaznego środowiska regulacyjnego, zgodnego

z europejskimi trendami, tj. w szczególności ograniczenia istniejących regulacji i uproszczenia czy wręcz zracjonalizowania systemu prawnego. Prace nad nowym reżimem prawnym dla sektora telekomunikacyjnego, czyli Digital Network Act, mogą w niedalekiej już przyszłości stać się naszą wspólną platformą do stworzenia przyjaznego otoczenia prawnego i systemu wyrównującego pozycję naszej branży w całym łańcuchu dostaw.



Problemy polskiego (mikro, małego, średniego) przedsiębiorcy telekomunikacyjnego



Paweł Wołoch
Prezes Zarządu
Związku Telewizji
Kablowych w Polsce
Izba Gospodarcza

Branża telekomunikacyjna w skali naszego kraju wydaje się być branżą zdecydowanie najbardziej przeregulowaną przez polskiego ustawodawcę. Nadmierne obowiązki sprawozdawczo-informacyjne, brak organizacji w ramach zbierania przez regulatora danych, nieuzasadniony wymóg udostępniania danych osobowych klientom końcowym dostawcy usługi medialnej sensu largo, ustawowa odpłatność za dostęp do sieci wewnątrzbudynkowej, nieadekwatne podstawy naliczania kar, a wreszcie niekorzystne przepisy prawno-autorskie, piętrzą dodatkowe trudności w prowadzeniu biznesu. Projektowane nowe przepisy (w tym uKSC) nie napawają optymizmem. Rząd powołał właśnie kolejną komisję ds. deregulacji, ale czy będzie ona efektywna i – co najważniejsze – weźmie pod uwagę głosy branży?

Wiele z nałożonych i nadal nakładanych na przedsiębiorców telekomunikacyjnych obowiązków winno ulec ograniczeniu lub wręcz zredukowaniu, do czego nieodzowna wręcz może okazać się poważna deregulacja, która jednakże może zostać wprowadzona wyłącznie drogą stosownych zmian przepisów rangi ustawowej.

Wprowadzając tego rodzaju zalecaną deregulację przede wszystkim trzeba odpowiedzieć sobie na pytanie czy te wszystkie dane, które są zbierane przez organy władzy i administracji publicznej od przedsiębiorców telekomunikacyjnych naprawdę w całości tym organom są bezwzględnie

niezbędne do realizacji zadań postawionych przed nimi przez ustawodawcę. Należałoby zrezygnować z dalszego zbierania tych danych, które nie są bezwzględnie niezbędne w prawidłowym realizowaniu zadań przez poszczególne organy władzy i administracji publicznej.

W odniesieniu z kolei do działalności ściśle telekomunikacyjnej (pomijamy zatem na razie działalność medialną sensu largo) przede wszystkim należałoby zrezygnować ze zbierania danych przez dwa organy administracji publicznej, scalając zbieranie tych danych i informacji „w rękach” jednego tylko organu, a mianowicie regulatora – Prezesa UKE.



Problemy polskiego (mikro, małego, średniego) przedsiębiorcy telekomunikacyjnego



Równie wskazane okazuje się ujednolicenie terminów realizowania obowiązków sprawozdawczo-informacyjnych poprzez przyjęcie jednego stałego terminu realizacji przez przedsiębiorców telekomunikacyjnych obowiązków sprawozdawczo-informacyjnych; okres sprawozdawczy powinien dotyczyć jednego roku kalendarzowego i być sprawozdawany przez przedsiębiorców telekomunikacyjnych regulatorowi do dnia 31 marca, co z kolei sprawi, że ingerencja ustawodawcy w terminy realizacji sprawozdawczości będzie najmniejsza z możliwych albowiem zdecydowana większość terminów sprawozdawania przewidzianych wobec przedsiębiorców telekomunikacyjnych opiewa na dzień 31 marca, poza jednym wyjątkiem, dotyczy poprzedniego roku kalendarzowego.

Zdecydowanie należałoby odstąpić od tego rodzaju wadliwej procedury zbierania danych w ramach różnych sprawozdań przez różne podmioty na rzecz zbierania pełnych danych jeden raz o tych samych usługach, czy też tych samych elementach infrastruktury.

W tym celu należałoby w jednym sprawozdaniu składanym jednemu organowi (regulatorowi) w jednym terminie scalić, póki co odrębnie, przekazywane dane:

1. o rodzaju i zakresie prowadzonej działalności telekomunikacyjnej i wielkości sprzedaży usług telekomunikacyjnych sprawozdawane Prezesowi UKE do 31 marca według stanu na 31 grudnia roku minionego (art. 20 pke), o usługach transmisji danych zapewniających szerokopasmowy dostęp do internetu sprawozdawanych samodzielnie oraz o tych samych usługach sprawozdawanych wraz ze świadczonymi w pakiecie usługami komunikacji głosowej oraz usługami rozprowadzania programów radiowych i telewizyjnych, które sprawozdawane są w ramach sprawozdawczości PIT do Prezesa UKE do 31 marca według stanu na 31 grudnia roku minionego (art. 29 ust. 2a pkt. 2 Megaustawy), o świadczonych lub planowanych do świadczenia w wyniku realizacji w ciągu 3 lat inwestycji realizowanych ze środków prywatnych w punktach adresowych za pomocą stacjonarnych lub ruchomych publicznych sieci telekomunikacyjnych usługach transmisji danych zapewniających stacjonarny szerokopasmowy dostęp do internetu sprawozdawanych w ramach systemu teleinformatycznego SIDUSIS do ministra właściwego do spraw informatyzacji do 10 dnia miesiąca za miesiąc poprzedni oraz, w przypadku większych podmiotów, co piątek (art. 29 j pkt. 1 i pkt. 3 Megaustawy w zw. z art. 29 k ust. 1 i ust. 4 Megaustawy),

2. posiadanej infrastruktury telekomunikacyjnej, posiadanych publicznych sieciach telekomunikacyjnych, przebiegu światłowodowych oraz innych niż światłowodowe linii kablowych zapewniających lub umożliwiających zapewnienie szerokopasmowego dostępu do internetu sprawozdawanych w ramach sprawozdawczości PIT Prezesowi UKE do 15 września za I półrocze danego roku i do 31 marca za II półrocze roku minionego (art. 29 ust. 2a pkt. 1 Megaustawy), obiektach budowlanych umożliwiających kolokację sprawozdawanych Prezesowi UKE w ramach sprawozdawczości PIT do 31 marca według stanu na 31 grudnia roku minionego (art. 29 ust. 2a pkt. 2 Megaustawy), oraz o infrastrukturze telekomunikacyjnej posiadanej przez przedsiębiorcę telekomunikacyjnego, niezbędnej do przygotowania systemów łączności na potrzeby obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego sprawozdawanej Prezesowi UKE do 31 marca według stanu na 31 grudnia roku minionego (art. 54 ust. 1 w zw. z art. 54 ust. 2 PKE).

Wielce pożądane byłoby także wprowadzenie prostej, niezwykle racjonalnej regulacji wedle której w sytuacji, gdy w zestawieniu z poprzednim okresem sprawozdawczym stan faktyczny objęty sprawozdawaniem zmianie nie uległ przedsiębiorca telekomunikacyjny nie byłby zobowiązany do składania jakichkolwiek oświadczeń, iż sprawozdawany za poprzedni okres sprawozdawczy stan faktyczny zmianie nie uległ.

Problemy polskiego (mikro, małego, średniego) przedsiębiorcy telekomunikacyjnego

Kolejnym racjonalnym postulatem jawi się oczekiwanie, aby w przypadku zmiany stanu faktycznego pomiędzy poszczególnymi okresami sprawozdawczymi nie zachodziła potrzeba sprawozdawania o całości usług lub infrastruktury czy też sieci, lecz sprawozdawaniem objęto by jedynie te dane, które uległy zmianie.

Z kolei podmiot świadczący usługę medialną sensu stricto będący osobą fizyczną i nie sporządzający sprawozdania finansowego winien przekazywać do KRRiT nie całe roczne zeznanie podatkowe, ale jedynie stanowiący załącznik do jego rocznego zeznania podatkowego PIT B dotyczący wyłącznie działalności gospodarczej przez taką osobę fizyczną prowadzonej.

Podmioty prowadzące działalność medialną sensu largo należałoby zwolnić z obowiązku zapewniania odbiorcom lub użytkownikom tych usług łatwego, stałego i bezpośredniego dostępu do imion i nazwisk członków wszelkich organów tych podmiotów, a także imion i nazwisk oraz nazw jakichkolwiek wspólników podmiotów świadczących usługi medialne sensu largo.

W sposób postulowany w niniejszym opracowaniu należałoby także zmienić regulacje dotyczące w największym stopniu spółdzielni mieszkaniowych, a więc nade wszystko normę art. 30 ust. 3a Megaustawy poprzez przyjęcie, że dostęp do wewnątrzbudynkowej infrastruktury telekomunikacyjnej będącej własnością podmiotu prowadzącego działalność telekomunikacyjną będzie także dla przedsiębiorcy telekomunikacyjnego zapewniany odpłatnie, oraz przepisy dotyczące



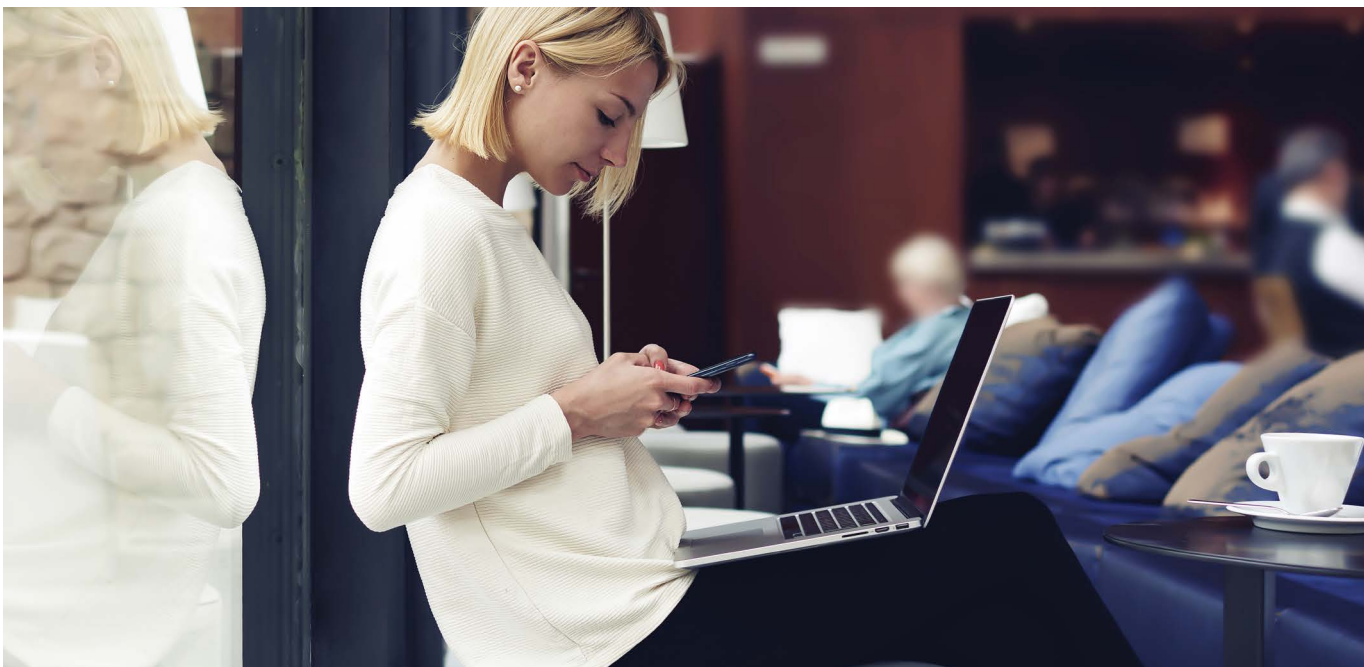
administracyjnych kar pieniężnych poprzez przyjęcie, że w odniesieniu do przedsiębiorców telekomunikacyjnych podstawę obliczenia administracyjnej kary pieniężnej będzie stanowił wyłącznie przychód z działalności telekomunikacyjnej tego podmiotu prowadzonej w roku minionym.

Wreszcie na gruncie przepisów prawnoautorskich należałoby wdrożyć właściwe regulacje prawne, a zatem:

- a. albo określić ustawą dla poszczególnych pól eksploatacji maksymalną wysokość opłat pobieranych od korzystających z utworów lub przedmiotów praw pokrewnych przez organizację zbiorowego zarządzania (ozz-y), które to opłaty zbierane by były przez ministra właściwego do spraw kultury i dziedzictwa narodowego, pozostawiając zarazem do rozstrzygnięcia w decyzji ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego określenie, któremu ozz-owi ile z tego wynagrodzenia pobranego od korzystającego na danym polu eksploatacji winno przypadać,

Problemy polskiego (mikro, małego, średniego) przedsiębiorcy telekomunikacyjnego

- b. albo też wprowadzić regulacje mocą których przewidziano by obowiązek posiadania przez ozz-y zatwierdzonych w trybie ustawowym tabel wynagrodzeń na polach eksploatacji, na których ozz-y te reprezentują prawa uprawnionych do utworów lub przedmiotów praw pokrewnych, przy jednoczesnym przewidzeniu sankcji na okoliczność nieposiadania zatwierdzonej w trybie ustawowym tabeli wynagrodzeń przez ozz pod postacią cofnięcia ozz-owi przez ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego zezwolenia na zbiorowe zarządzania prawami autorskimi lub prawami pokrewnymi na konkretnym polu eksploatacji, przy czym na tę okoliczność mocą zapisu ustawowego przewidziano by decyzję związaną ministra kultury i dziedzictwa narodowego nie zaś, jak to miało miejsce w latach 2010-2018 jedynie decyzję uznaniową tegoż ministra.



Postulowane przez nas w niniejszym opracowaniu zmiany ustawodawcze choćby w pewnym stopniu mogłyby przyczynić się do nieznacznego odciążenia przedsiębiorców od realizacji ciężących na nich obowiązków, jak i wpłynęłyby na eliminowanie z obrotu prawnego pewnych wielce niekorzystnych dla przedsiębiorców telekomunikacyjnych regulacji natury prawnej.

Wprowadzenie przedmiotowych zmian w nieodległej perspektywie czasowej mogłoby także przyczynić się do zapewnienia rozwoju branży telekomunikacyjnej w wyniku sprawniejszego, na jeszcze wyższym poziomie jakościowym, świadczenia usług telekomunikacyjnych przez przedsiębiorców

telekomunikacyjnych. Przedsiębiorca ten nie musiałby w tak znaczącym stopniu angażować swoich pracowników i współpracowników do realizacji nad wyraz rozrośniętych obowiązków sprawozdawczo-informacyjnych obejmujących różne okresy rozliczeniowe realizowane w różnych przedziałach czasowych. Pozwoliłoby to na skierowanie aktywności osób zatrudnionych przez operatora w większym stopniu na zajmowanie się świadczeniem usług telekomunikacyjnych, a w mniejszym na wykonywanie czynności sprawozdawczo-informacyjnych wobec organów władzy i administracji publicznej.

Problemy polskiego (mikro, małego, średniego) przedsiębiorcy telekomunikacyjnego

Proponowane regulacje obniżyłyby także koszty prowadzenia działalności gospodarczej. Przy tak olbrzymim obciążeniu obowiązkami sprawozdawczo-informacyjnymi jak obecnie pracownicy niezależnie od wykonywania czynności sprawozdawczo-informacyjnych i tak muszą zajmować się też realizacją przedmiotu działalności telekomunikacyjnej. W praktyce nierzadko te same osoby zajmują się także obsługą klientów, przyjmowaniem płatności, procedurą podpisywania umów, podłączaniem i odłączaniem abonentów, usuwaniem awarii i usterek, monitorowaniem sieci, a to tylko niektóre czynności składające się na prowadzenie działalności telekomunikacyjnej.

Mając na uwadze specyfikę prowadzenia działalności telekomunikacyjnej przedsiębiorca telekomunikacyjny za dodatkowe zaangażowanie pracowników nie posiada możliwości udzielenia im w innym czasie czasu wolnego od pracy za pracę w godzinach nadliczbowych (art. 1512 § 1 k.p. w zw. z art. 1512 § 2 k.p.), co implikuje potrzebę wypłaty pracownikom za pracę w godzinach nadliczbowych poza normalnym wynagrodzeniem za czas dodatkowo przepracowany także dodatku za pracę w godzinach nadliczbowych w wysokości 50% lub 100% zasadniczego wynagrodzenia konkretnego pracownika (art. 1512 § 3 k.p. w zw. z art. 1511 § 1 k.p. w zw. z art. 1511 § 2 k.p.). Zwiększa to i tak już niemałe koszty pracodawcy ponoszone w związku z realizacją przez niego działalności telekomunikacyjnej.

Wskazane propozycje zmian ustawowych to tylko wierzchołek góry lodowej albowiem zmian dotyczących funkcjonowania przedsiębiorców telekomunikacyjnych winno być o wiele więcej. W artykule ograniczyłem się do wymienienia jedynie najpoważniejszych i najczęstszych problemów dotyczących mikro, małego i średniego przedsiębiorcy telekomunikacyjnego (wiele z tych problemów dotyka także dużych przedsiębiorców telekomunikacyjnych).

Przedstawione propozycje stanowią pewnego rodzaju remedium na stwierdzone bolączki. Pytanie, czy władze naszego kraju będą skłonne ugiąć się przed postulatami rynku, których akceptacja mogłaby przyczynić się chociażby w pewnym stopniu do ulżenia wyjątkowo ciężkiej sytuacji polskiego przedsiębiorcy telekomunikacyjnego na naszym polskim rynku usług telekomunikacyjnych.



Telekomy w nowym Krajowym Systemie Cyberbezpieczeństwa



Piotr Kowalski
Manager ds.
Transformacji
Orange

Nie ma tygodnia, żebyśmy nie słyszeli o uproszczeniu regulacji prawnych, które mają ułatwić prowadzenie działalności gospodarczej i pomóc znaleźć nowe silniki rozwoju gospodarki narażonej na coraz więcej wstrząsów. Ta narracja już oficjalnie zagościła do unijnych i krajowych dokumentów strategicznych. Ba, jako przedsiębiorcy sami do niej nawołujemy. Bo jest po prostu obiektywnie potrzebna.

Jednak w tle regulacja zatacza coraz szersze kręgi i obejmuje nowe obszary działania firm. Jednym z lepszych przykładów jest tak zwane cyberbezpieczeństwo, które jeszcze kilka lat temu było domeną specjalistycznych zespołów, które kierując się wiedzą, doświadczeniem i dostępnym budżetem starały się jak najlepiej zabezpieczyć działalność firmy. Te czasy się skończyły.

Świadomość i dostosowanie do nowych obowiązków będą niezbędne, aby w przyszłości nie obawiać się kontroli oraz utrzymać atrakcyjność usług dla klientów.



Od bezpieczeństwa i integralności sieci oraz usług do cyberbezpieczeństwa

W sektorze telekomunikacyjnym – zarówno wśród mniejszych jak i większych operatorów – dobrze znamy wymagania dotyczące bezpieczeństwa lub integralności sieci lub usług wynikające z prawa telekomunikacyjnego i wydanych do niego rozporządzeń. Będą one obowiązywały do czasu rozpoczęcia stosowania nowych ram, które określi nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC). Prace nad nią trwają od września 2020 i wciąż trudno określić, kiedy zostaną zakończone. Wiemy, że mają wejść w życie po 30 dniach od publikacji w Dzienniku Ustaw i od tego momentu rozpocznie się 6-miesięczny termin na osiągnięcie zgodności. Biorąc pod uwagę zakres wymagań okres ten jest bardzo krótki. W przyjętej w maju implementacji NIS2 w Belgii na wdrożenia przewidziano 18 miesięcy.

Kogo obejmą nowe wymagania?

Aktualnie wymagania KSC dotyczą przede wszystkim 378 wyznaczonych decyzjami administracyjnymi operatorów usług kluczowych. Dotyczą także szerokiego spektrum podmiotów publicznych oraz dostawców usług cyfrowych. Telekomunikacja jest wprost wyłączona z tego zakresu. Obszarem związanym z telekomunikacją i objętym ksc są natomiast największe punkty wymiany ruchu internetowego (IXP).

Nowe przepisy mają według szacunków Ministerstwa Cyfryzacji objąć ok. 10 tys. firm i 28 tys. jednostek publicznych, w tym samorządy. Ta skala już od dawna rozbudza wyobraźnię zarówno po stronie regulowanych podmiotów, jak i dostawców rozwiązań organizacyjnych, sprzętowych i oprogramowania. Będzie też miała swoje skutki w łańcuchach dostaw.



Wymagania uKSC

- Samoidentyfikacja i wpis do rejestru podmiotów kluczowych i ważnych
- Korzystanie z systemu s46 (art. 46) służącego komunikacji w ramach KSC
- Wdrożenie systemu zarządzania bezpieczeństwem informacji (SZBI), w tym szacowania ryzyka oraz środków techniczno-organizacyjnych
- Określenie kierownika podmiotu jako odpowiedzialnego
- Weryfikacja personelu wykonującego zadania (SZBI i zgłaszanie incydentów) pod kątem skazania za przestępstwa przeciwko ochronie informacji
- Wyznaczenie 2 osób (1 dla mikro i małych) do kontaktu z podmiotami KSC
- Opracowanie i utrzymanie dokumentacji normatywnej i operacyjnej
- Zgłaszanie incydentów poważnych: 24 godziny na przekazanie wczesnego ostrzeżenia, 72 na zgłoszenie, miesiąc na sprawozdanie końcowe
- Informowanie klientów
- Powołanie wewnętrznych struktur do realizacji zadań lub zawarcie umowy z dostawcą usług zarządzanych cyberbezpieczeństwa
- Przeprowadzenie audytu raz na 3 lata (tylko podmiot kluczowy)

Średni i duzi przedsiębiorcy komunikacji elektronicznej będą włączeni do KSC jako podmioty kluczowe. Mikro i mali przedsiębiorcy będą rozpoznawani jako podmioty ważne. W praktyce oznacza to niemal ten sam zestaw ramowych wymagań dotyczących wdrożenia i utrzymania systemu zarządzania bezpieczeństwem informacji. Różnice dla mikro i małych firm sprowadzają się do braku obowiązku prowadzenia regularnych audytów oraz stosowania łagodniejszych narzędzi kontrolnych.

Czy trzeba osiągnąć zgodność z NIS2 czy KSC?

Dyrektywa NIS2 weszła w życie w styczniu 2023, a termin na jej przeniesienie do krajowych przepisów upłynął w październiku 2024. Dla polskich firm ma to jednak ograniczone skutki praktyczne. Zasady i terminy osiągnięcia zgodności będą wynikały z krajowej ustawy, tj. ustawy o krajowym systemie cyberbezpieczeństwa oraz wydanych do niej rozporządzeń. Dzisiaj można szacować, że data końcowa przypadnie w pierwszym kwartale 2026. Podobnie jak w przypadku Europejskiego Kodeksu Łączności Elektronicznej, który do stosowania włączyły krajowe przepisy, w tym szczególnie Prawo Komunikacji Elektronicznej i jego ustawa wprowadzająca. Treść NIS2 i projektu uKSC mogą być jednak wskazówką jak zawczasu przygotowywać się do nadchodzących zmian.

A jeśli mam więcej „cyfrowych” PKD?

Dla niektórych firm telekomunikacyjnych działalność ta nie jest jedynym strumieniem biznesowym. Dlatego warto zweryfikować swój zakres działania z NIS2 i załącznikami do projektowanej nowelizacji KSC.



Regulowana będzie bowiem też aktywność np. w zakresie: centrów danych, dostawców usług chmurowych, CDN, usług zarządzanych ICT i cyberbezpieczeństwa. Między innymi dla takich usług Komisja Europejska wydała szczegółowe rozporządzenie określające progi dla zgłoszeń incydentów oraz wymagania techniczne i metodyczne, które na 28 stronach doprecyzowują co należy uwzględnić. Te przepisy do stosowania w Polsce również wprowadzi krajowa nowelizacja KSC.

Telekomy w nowym Krajowym Systemie Cyberbezpieczeństwa

Co na to nasi klienci? O nieoczywistym wpływie pośrednim

Skala stosowania nowego KSC będzie niewątpliwie szeroka. To co jednak dla firm telekomunikacyjnych i szerzej „cyfrowych” będzie szczególnie istotne to, że nasi klienci będący także regulowani w nowym KSC powinni uwzględnić wpływ swoich bezpośrednich dostawców w ocenie ryzyka. Już dzisiaj można przewidzieć, że jednym z większych wyzwań organizacyjnych będzie wzajemne potwierdzanie właściwego stosowania wymagań i pożądanых praktyk bezpieczeństwa. Same telekomy też muszą zrobić to dla swoich zasobów. Dlatego korzystanie z usług – także w usługach hurtowych – podmiotów, które stosują najlepsze praktyki, w tym posiadają własne CERT, SOC, NOC oraz certyfikację ISO 27001 i 22301 może okazać się w przyszłości pomocne.



Wybrane uprawnienia podmiotów

- Skoordynowane ujawnianie podatności prowadzone przez CSIRT NASK
- Wnioskowanie o przekazanie informacji technicznych o incydentach
- Rekomendacje Pełnomocnika Rządu ds. Cyberbezpieczeństwa oraz badanie produktów lub usług ICT przez CSIRT
- Ocena bezpieczeństwa systemów informacyjnych prowadzona przez CSIRTy
- Wezwanie do usunięcia podatności
- Nadzór stosowania przepisów i prowadzenie kontroli oraz wykonywanie szczególnych uprawnień wobec podmiotów kluczowych
- Żądanie przekazania wszelkich informacji i dokumentów dot. stosowania ustawy, w tym tłumaczeń dokumentacji
- Publikacja zestawienia norm realizujących wymagania ustawy
- Wyznaczenie urzędnika monitorującego
- Analiza produktów, usług lub procesów ICT i decyzja w sprawie dostawcy wysokiego ryzyka
- Wydawanie rekomendacji dot. środków technicznych i organizacyjnych
- Wydawanie poleceń zabezpieczających
- Kary pieniężne, w tym dla kierownika podmiotu

Trudno będzie się prześlizgnąć, czyli o uprawnieniach organów kontroli

Nowelizacja KSC przyniesie też unikalny zestaw narzędzi kontrolnych dla organów administracji. Dla komunikacji elektronicznej organem właściwym – odpowiedzialnym za monitorowanie stosowania przepisów ustawy – będzie Prezes Urzędu Komunikacji Elektronicznej. W 18 miesięcy od wejścia w życie ustawy ma on powołać CSIRT sektorowy. Zarówno podmioty kluczowe, jak i ważne będą zobowiązane do przekazywania wszelkich informacji dotyczących wykonywania obowiązków ustawowych.

Prezes UKE będzie zaś miał możliwość ich weryfikacji oraz określania sposobu zapewnienia zgodności oraz nakładania kar, w tym finansowych za naruszenia. Szczególnym, nowym uprawnieniem będzie też możliwość wydania przez Ministra ds. Informatyzacji (aktualnie Minister Cyfryzacji) polecenia zabezpieczającego, które w przypadku incydentów zakwalifikowanych przez właściwy CSIRT krajowy (NASK, GOV lub MON) jako krytyczne, może zawierać daleko idące nakazy określonego zachowania, w tym dotyczące konfiguracji systemów lub wdrożenia innych środków zaradczych.

Telekomunikacja też podjęła rękawicę rzuconą przez premiera



Joanna Sikora
Koordynator
Międzyzbowego
Zespołu
Telekomunikacyjnego
ds. Deregulacji

Pod koniec lutego tego roku rozpoczął pracę Zespół Deregulacyjny Rafała Brzosi, powołany przez premiera. W celu realizacji założeń zespołu, Fundacja Rafała Brzosi rozpoczęła gromadzenie ekspertów a następnie prace merytoryczne w ramach inicjatywy deregulacyjnej „SprawdzaMy”. Inicjatywa jest krokiem w kierunku uproszczenia przepisów prawnych i zmniejszenia obciążeń biurokratycznych dla przedsiębiorców w Polsce. Jej celem jest zdefiniowanie i usunięcie przepisów prawa stanowiących nadregulację i obciążenie w prowadzeniu działalności gospodarczej przez przedsiębiorców.

Deregulacja, szczególnie w telekomunikacji, która od lat jest przeregulowana, ma na celu stworzenie bardziej sprzyjających warunków dla rozwoju usług telekomunikacyjnych, poprzez eliminację niepotrzebnych, zbędnych i nadmiarowych regulacji. Dlatego branża telekomunikacyjna aktywnie włączyła się w tę Inicjatywę już od pierwszych jej dni.

Pierwszym krokiem, do jak się okazało, bardzo efektywnej współpracy, było powstanie Telekomunikacyjnego Zespołu Deregulacyjnego. Zainicjowała go Anna Streżyńska, członkini Zarządu Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji, jednocześnie jeden z ekspertów Rady ekspertów ds. cyfryzacji, rozwoju oraz wsparcia badań.



Tym samym, prawie jednocześnie z powstaniem Inicjatywy SprawdzaMy, powstał Telekomunikacyjny Zespół Deregulacyjny. Tworzy go 7 podmiotów, zrzeszających małych i dużych przedsiębiorców telekomunikacyjnych reprezentujących różne, bardzo często konkurencyjne wobec siebie interesy. To jednak nie stało na drodze do efektywnej i merytorycznej współpracy. Jej celem jest wprowadzenie oczekiwanych od lat przez cały rynek telekomunikacyjny zmian, które pozytywnie odczują wszyscy przedsiębiorcy telekomunikacyjni, a w efekcie końcowym również użytkownicy końcowi.

W skład Zespołu Telekomunikacyjnego weszło ponad 40 osób, przedstawicieli przedsiębiorców telekomunikacyjnych, ekspertów, którzy z dużym zaangażowaniem wspólnie definiują bariery, problemy i poszukują rozwiązań, wspierających cyfryzację i rozwój telekomunikacji w Polsce. Cotygodniowe spotkania Zespołu stanowią przestrzeń do wnikliwej, merytorycznej dyskusji i wypracowywania konsensusu w postaci konkretnych propozycji zmian przepisów – „antidotum” dla problemów zgłaszanych nie tylko przez samych przedsiębiorców telekomunikacyjnych, ale również przez osoby postronne w ramach samej Inicjatywy SprawdzaMy.

Telekomunikacja też podjęła rękawicę rzuconą przez premiera

Dla postulatu zmiany przepisów, który znajduje uznanie wszystkich członków Zespołu, przygotowywana jest tzw. "formatka", czyli dokument zawierający opis problemu, uzasadnienie konieczności zmiany oraz konkretne propozycje legislacyjne, które stanowią jego rozwiązanie. Tytuł postulatu odzwierciedla istotę zmiany, jaką ma wprowadzić, oraz wskazuje obszar, który ma zostać poprawiony lub uproszczony. Wyzwaniem jest opisanie problemów telekomunikacyjnych tak, by każdy mógł łatwo zrozumieć, jak proponowane zmiany mogą wpłynąć na branżę telekomunikacyjną, a także abonentów.

Celem Zespołu było w pierwszej kolejności przedłożenie propozycji zmian, mających skutkować usunięciem barier inwestycyjnych, co powinno przełożyć się na lepszą jakość usług telekomunikacyjnych, niższe koszty oraz szybszy rozwój sektora.

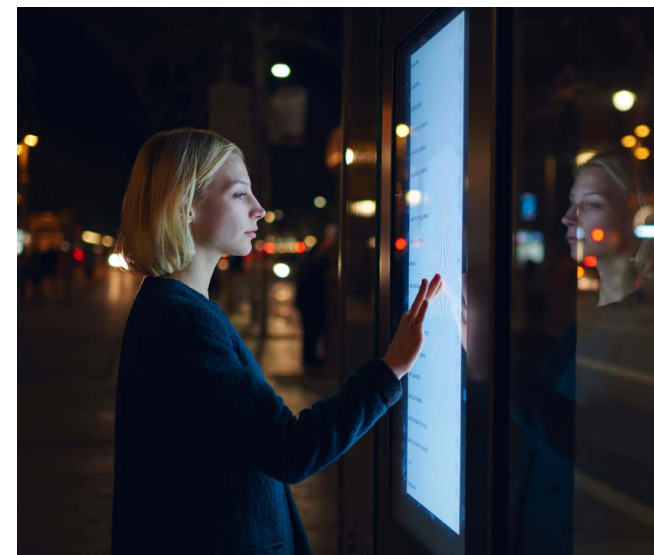
Najlepszym dowodem determinacji i skuteczność działań Zespołu są 33 postulaty zmian przepisów dotyczących telekomunikacji, które zostały przygotowane i przekazane Inicjatywie Sprawdzamy. 30 z tych postulatów zostało złożonych już 2 marca 2025 r., a więc zaledwie kilka dni od powstania samej Inicjatywy. Postulaty te dotyczą m.in. właśnie definiowanych od lat barier inwestycyjnych w telekomunikacji, tj. zmian w ustawie: prawo komunikacji elektronicznej, megaustawa, prawo budowlane, o drogach publicznych, itd., w celu stworzenia bardziej sprzyjających warunków dla inwestycji w infrastrukturę telekomunikacyjną, co jest kluczowe dla dalszego rozwoju tej branży. Co więcej, likwidacja barier inwestycyjnych, zwłaszcza poprzez zmiany w kluczowych ustawach, to krok w stronę stworzenia bardziej sprzyjającego środowiska dla rozwoju infrastruktury telekomunikacyjnej.

Obecnie 18 z 33 postulatów przekazanych przez Zespół Telekomunikacyjny do Inicjatywy Sprawdzamy zostało już opublikowanych na stronie <https://sprawdzamy.com/> pod tytułami:

1. Tańsza i łatwiejsza rozbudowa sieci telekomunikacyjnych
2. Lepszy internet i szybka rozbudowa sieci – bez zbędnych formalności
3. Szybsza rozbudowa sieci – mniej formalności, więcej internetu
4. Szybsza budowa sieci telekomunikacyjnych – koniec z długim oczekiwaniem
5. Szybszy dostęp do internetu – mniej formalności dla operatorów
6. Telekomunikacja bez barier – szybkie inwestycje dzięki prostszym procedurom
7. Koniec z biurokracją w telekomunikacji – jeden system raportowania i proste procedury

Każda propozycja została przedstawiona w sposób jasny i przystępny. Można się z nimi zapoznać po wejściu w link: <https://sprawdzamy.com/zgloszone-pomysly?categories=telekomunikacja> i zgłaszać na pomysł, który się popiera lub go skomentować, co pozwala na aktywny udział społeczności w tym procesie. To bardzo ważny element tej inicjatywy, który sprzyja większej akceptacji i skuteczności proponowanych zmian. Dzięki temu proces staje się bardziej transparentny i demokratyczny. Obecnie na inicjatywy telekomunikacyjne zostało oddanych już ponad 9000 głosów obywateli.

Do jednego z cotygodniowych spotkań Zespołu Telekomunikacji dołączył Prezes Rafał Brzoska, który podziękował za pracę, zaangażowanie,



profesjonalizm i kompletność dokumentów przygotowanych przez Zespół Telekomunikacyjny, który – jak sam wskazał – jest najbardziej efektywnym zespołem w ramach Inicjatywy.

Dzięki Inicjatywie Sprawdzamy oraz zgodnej współpracy całej branży, sektor telekomunikacyjny zyskuje realną szansę na uproszczenie przepisów i eliminację zbędnej biurokracji, a abonenci – na poprawę jakości usług oraz większą dostępność nowoczesnych technologii. Dlatego Zespół Telekomunikacyjny nie spoczywa na laurach i pracuje nad kolejnymi propozycjami zmian, z którymi sukcesywnie będzie można się zapoznać na stronie <https://sprawdzamy.com/>.

Jeśli przychodzą Państwu na myśl problemy, które sami widzicie i zależy Wam na ich usunięciu zachęcam do ich zgłoszenia do Zespołu Telekomunikacyjnego.

Od legislacyjnej teorii do rynkowej praktyki. Walka z CLI spoofingiem



Agnieszka Grabowska
Kierownik Wydziału
Zarządzania Ochroną
Przychodów i Nadużyć
Orange



Marcin Bystrowski
Ekspert ds. Ochrony
Przychodów i Nadużyć
Telekomunikacyjnych
Orange

Historia oszustwa

Zjawisko podszywania się (spoofingu) pod inny numer telefonu (Calling Line Identification) jest starsze niż mogłoby się wydawać. Dziś kojarzy się głównie z zaawansowanymi oszustwami, ale początki tej praktyki sięgają znacznie dalej.

Pierwsze przypadki podmieniania numerów pojawiły się wraz z rozwojem telefonii stacjonarnej. W tamtych czasach było to znacznie trudniejsze technicznie i wiązało się z ingerencją w złożoną infrastrukturę telekomunikacyjną. Motywacje przestępców były różne: od zwykłych żartów po poważne przestępstwa.

Znaczny wzrost CLI spoofingu nastąpił w ostatnich latach. Zmiana numeru wyświetlanego na ekranie odbiorcy stała się znacznie łatwiejsza i tańsza. Oszuści zaczęli wykorzystywać tę technikę do wprowadzenia odbiorcy w błąd, co do swojej tożsamości lub lokalizacji. W połączeniu z socjotechniką ułatwiło to im dokonywanie różnego rodzaju wyłudzeń m.in.: „Metodą na wnuczka”, „Fałszywego pracownika banku” czy też „Wyłudzenie na policjanta”.



Nowe prawo w walce z oszustami

W Polsce CLI spoofing jest zabroniony prawnie. Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej (UZNKE) z 25 września 2023 roku nakłada na wszystkich przedsiębiorców telekomunikacyjnych obowiązek stosowania środków technicznych i organizacyjnych, które mają na celu wykrywanie i blokowanie połączeń o charakterze CLI spoofingu.

Ustawa dokładnie określa, jakie zachowania są uważane za nadużycia w komunikacji elektronicznej. Operatorzy telekomunikacyjni mają teraz większe uprawnienia do blokowania połączeń podejrzanych o nadużycia. Ustawa umożliwia też współpracę między operatorami, co pozwala na szybszą reakcję na nowe zagrożenia. Dzięki temu łatwiej jest zidentyfikować i wyciągnąć konsekwencje wobec sprawców.



Dzisiaj nawet 1,2% przeanalizowanych połączeń głosowych jest klasyfikowanych jako spoofing.

Od legislacyjnej teorii do rynkowej praktyki. Walka z CLI spoofingiem

Jak wykryć fałszerza

Orange stosuje bardzo zaawansowane technologie, aby wykrywać i blokować podejrzane połączenia, które mogą być związane ze CLI spoofingiem.

W ramach walki ze spoofingiem powstało porozumienie tzw. „bezpieczna zatoka”. Jest to unikalne rozwiązanie techniczne, które zostało opracowane przez największych operatorów telekomunikacyjnych w Polsce, we współpracy z Urzędem Komunikacji Elektronicznej (UKE). Stworzony system antyspoofingowy jest innowacją na skalę światową i pierwszym tak działającym systemem weryfikującym połączenia.



W ramach „bezpiecznej zatoki” operatorzy nawzajem wspierają się w zwalczaniu spoofingu i wymieniają się potrzebnymi informacjami.

Mechanizm jest tak skonstruowany, że sprawdzanie odbywa się w bardzo krótkim czasie podczas zestawiania połączenia. Jeśli system wykryje, że mamy do czynienia z próbą podmiany numeru, połączenie może zostać odrzucone lub zestawione, ale bez wyświetlania numeru dzwoniącego (zostanie wyświetlony komunikat "Numer nieznany"). Klient odbierający połączenia, nie ma świadomości ochrony, jaką zapewnia mu jego operator.

Porozumienie jest dostępne dla wszystkich operatorów telekomunikacyjnych, którzy obsługują co najmniej 50 tys. abonentów i są gotowi spełnić określone wymagania techniczne. Pozostali operatorzy korzystają z rekomendacji UKE.

Nowe zagrożenia na horyzoncie

Aby skutecznie chronić się przed CLI spoofingiem, należy być świadomym zagrożeń i stosować podstawowe zasady bezpieczeństwa. Mimo tych działań, nadużycia pozostają poważnym problemem, a oszuści wciąż wymyślają nowe, coraz bardziej wyrafinowane metody.

Przy pomocy sztucznej inteligencji, przestępcy potrafią wygenerować niezwykle realistyczne imitacje głosów (deepfake) znanych osób, aby przekonać ofiary do ujawnienia poufnych informacji. Połączenie deepfaków głosowych z wideo pozwala na tworzenie jeszcze bardziej przekonujących oszustw. Przestępcy mogą przeprowadzać wideo rozmowy, w których podszywają się pod bliskich, współpracowników czy przedstawicieli instytucji państwowych. Dzięki temu ataki stają się jeszcze bardziej wiarygodne i trudniejsze do wykrycia.

Współpraca i edukacja kluczem do sukcesu

Ustawa daje operatorom podstawy prawne do działań. Rozwiązania techniczne umożliwiają wykrywanie nadużyć, ale walka z CLI spoofingiem tutaj się nie kończy. Wymaga ona ciągłego doskonalenia technologii. Może też być jeszcze skuteczniejsza, jeśli zadbamy o edukację społeczeństwa, współpracę między różnymi podmiotami oraz wszyscy będziemy pamiętać o zasadzie ograniczonego zaufania.

Chińskie Mury w pomarańczowym kolorze



Jolanta Steppa
Manager
ds. Transformacji
Orange

Każdy słyszał o Chińskim Murze, który miał bronić Chin przed najazdami koczowniczych ludów, takich jak Xiongnu, czy Mongołowie. Nie wszyscy jednak wiedzą, że Chińskie Mury istnieją także w Orange Polska. W przeciwieństwie do Chin, nie stosujemy ich dla ochrony przed konkurentami, ale jako specjalne zabezpieczenia, które wprowadziliśmy do ochrony interesów naszych klientów hurtowych.

Chińskie Mury to nazwa systemów chroniących informacje o klientach, które firmy pozyskują w ramach świadczonych usług. Są to zabezpieczenia systemowe, informatyczne, jak również „kulturowe”. Strzegą przed wykorzystywaniem tych danych do innych celów, m.in. dla osiągnięcia przewagi konkurencyjnej na innych rynkach.

W ramach współpracy międzyoperatorskiej Orange posiada informacje o usługach detalicznych świadczonych przez swoich klientów hurtowych. Jednocześnie sam świadczy usługi detaliczne. Chińskie Mury wprowadziliśmy właśnie dlatego, aby nie dochodziło do niewłaściwego wykorzystywania tych informacji. Na rynku detalicznym gramy fair play, nie wykorzystując danych, które pozyskaliśmy przy okazji świadczenia usług hurtowych.

Tradycja Chińskich Murów w Orange sięga jeszcze 2009 roku, kiedy potwierdziliśmy ich zasady z regulatorem, w specjalnym porozumieniu. Pomimo, że porozumienie obowiązywało przez 3 lata, do dziś chronimy dane klientów zgodnie z jego zapisami.



Chińskie Mury w pomarańczowym kolorze

1. Chińskie Mury to polityka całej firmy, wspierana przez Zarząd, który na podstawie specjalnych uchwał, przyjął dwa kluczowe dokumenty w zakresie Chińskich Murów, tj.
 - a. Regulamin Chińskich Murów – określający zbiór zasad ochrony informacji o klientach hurtowych i przestrzegania Chińskich Murów w firmie,
 - b. Katalog kategorii Danych Chronionych objętych Chińskimi Murami – czyli wykaz informacji o naszych klientach hurtowych (i ich klientach detalicznych), które podlegają ścisłej ochronie.

2. Orange podzielony został na trzy podstawowe domeny:

- a. Hurt,
- b. Detal,
- c. Korpo (funkcje wsparcia, nie zaangażowane biznesowo ani w sprzedaż detaliczną, ani hurtową).

Ten podział pozwala także informatycznie zarządzić dostępem do informacji. Jeśli masz domenę Detal nie dostaniesz dostępu do systemu informatycznego, w którym znajdują się dane dotyczące klientów hurtowych.

3. Ograniczenia dostępu do danych nie dotyczą tylko systemów informatycznych. Zakaz przekazywania takich danych dotyczy wszelkich form ich udostępniania czy przetwarzania – czy to na oficjalnym spotkaniu w firmie, czy na kawie z kolegą.

4. Dane mają swoich biznesowych właścicieli, odpowiedzialnych za ich ochronę. Dodatkowo pracownicy naszej firmy są zobowiązani do zgłaszania wszelkich incydentów związanych z podejrzeniem naruszenia Chińskich Murów. Dane sygnalistów są chronione, co ma zachęcać do takich zgłoszeń.

5. Cyklicznie przypominamy naszym pracownikom o zasadach dostępu do informacji poprzez szkolenia. Co więcej, wymagamy, aby zasady Chińskich Murów były stosowane nie tylko przez pracowników, ale także przez naszych współpracowników.

6. Aby zapewnić prawidłowe funkcjonowanie systemu Chińskich Murów, Zarząd powołał Administratora Chińskich Murów. To on nadzoruje system, udziela dodatkowych wytycznych w mniej oczywistych sprawach, ale także przyjmuje i rozpatruje skargi czy zgłoszenia od sygnalistów.

Jako firma mamy niewątpliwie największe doświadczenie na polskim rynku telekomunikacyjnym w stosowaniu Chińskich Murów i ochronie danych naszych klientów hurtowych. Ochrona ta zaszyta jest nie tylko w naszych umowach, systemach informatycznych, ale można wręcz stwierdzić, że jest w DNA naszej firmy. Wierzmy, że odpowiedzialne wykorzystanie danych wrażliwych oraz ich zabezpieczenie na najwyższym poziomie jest kluczowe dla budowania zaufania i owocnej współpracy biznesowej.



3 Odporność sieci

- Dezinformacja w telekomunikacji
- Zagrożenia militarne
- Niebezpieczne zmiany klimatyczne



Odporność sieci: dezinformacja w telekomunikacji



Mateusz Madejski
Ekspert ds.
Prawnych i Regulacji
Orange

Telekomunikacja po prostu ma być – dla wygody, przyjemności, bezpieczeństwa czy produktywności. Z punktu widzenia użytkownika liczy się to, że po włączeniu komputera czy smartfona jesteś w sieci. Jak to się dzieje, że urządzenie momentalnie łączy się z całym światem? Przeciętnego użytkownika to nie interesuje tak długo, jak sieć magicznie działa poza zasięgiem jego wzroku. Wiemy jednak, że aby zapewnić łączność, potrzebna jest realna infrastruktura, którą trzeba wybudować i o którą należy dbać. I tu często zaczynają się problemy.



Procedury budowlane w Polsce są już wystarczająco skomplikowane i czasochłonne, a dodatkowo operatorzy często muszą zmagać się z oporem lokalnych społeczności. Przecież sieć ma być niewidoczna – dlaczego więc każecie mi patrzeć przez okno mojego domu na jakąś wieżę? A zresztą, czy to bezpieczne, że taka antena tam wisi i coś emituje? Jak wynika z **badń** przeprowadzonych w 2024 roku przez Katolicki Uniwersytet Lubelski na zlecenie Polskiej Izby Informatyki i Telekomunikacji, aż 42% ankietowanych w Polsce nie zgodziłoby się na budowę nadajnika sieci komórkowej w promieniu 500 m od swojego miejsca zamieszkania. Co ciekawe, taki brak zgody w równoległe przeprowadzonych badaniach w Niemczech i Japonii wyrażało tylko, odpowiednio, 31% i 7% ankietowanych. W tych okolicznościach inwestycje faktycznie służące interesom Polaków bywają przez nich uznawane za źródło zagrożenia.

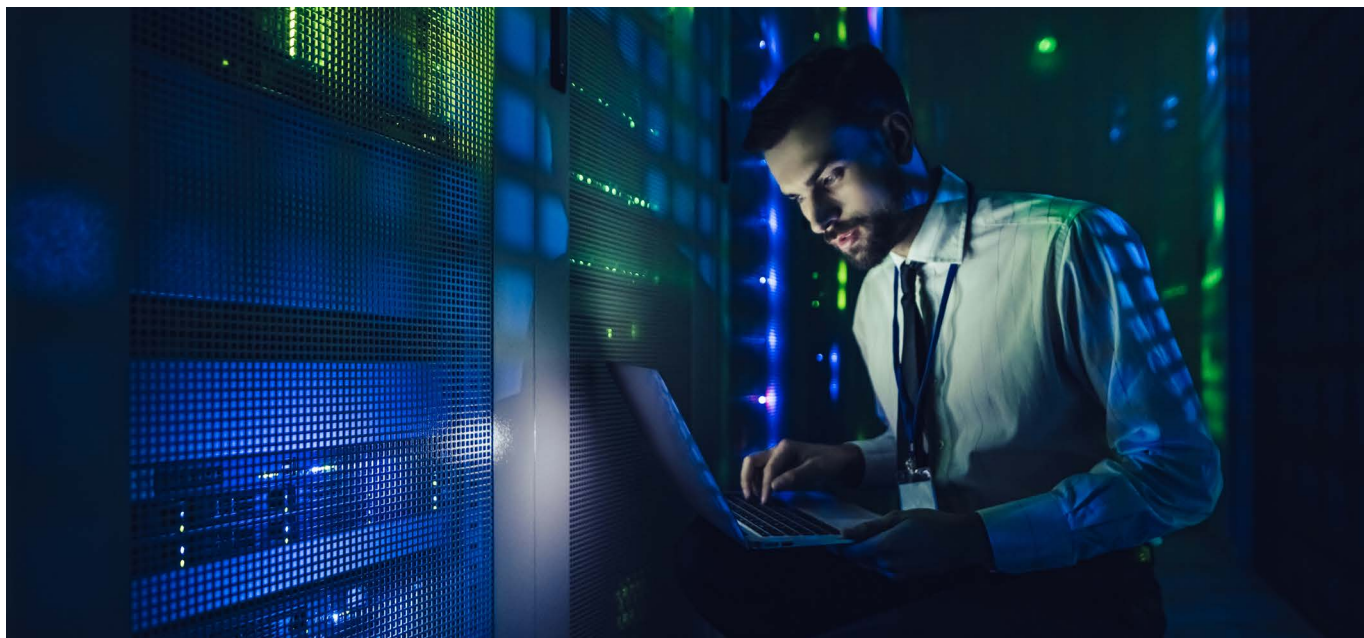
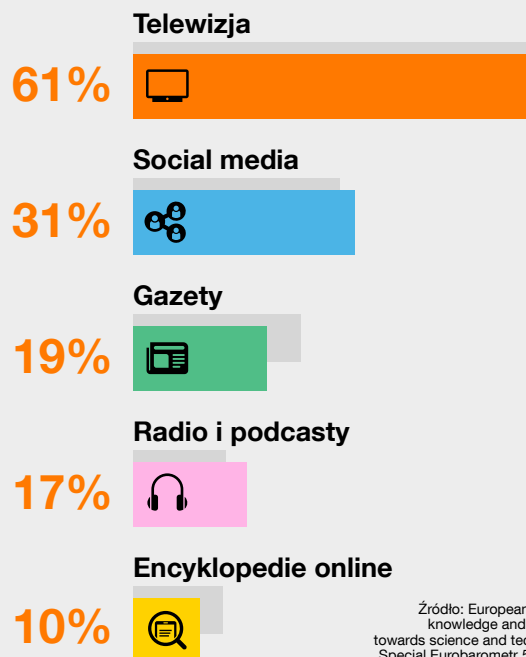
Wyławianie ludzi zagubionych w morzu informacji

Osoby specjalizujące się w dezinformowaniu społeczeństwa wykorzystają każdą okazję, by zagospodarować niechęć, niepokój i brak wiedzy. Skoro dla kogoś niezainteresowanego technologią działanie sieci jest pełne tajemnic, to nietrudno jest przekonać go, że operatorzy uprawiają czarną magię. Oczywiście infrastruktura musi spełniać – i spełnia – wyśrubowane normy środowiskowe opracowane na bazie wieloletnich ustaleń naukowych, co do których w środowisku naukowym panuje konsensus. Mimo to wraz z pojawieniem się technologii 5G jak grzyby po deszczu wyrosły teorie spiskowe o szkodliwości telefonii komórkowej. Siewcy dezinformacji nie poprzestali na żerowaniu na przyziemnych (i nieuzasadnionych) obawach, jak te związane z domniemanymi przyczynami ciężkich chorób. Po sieci zaczęły krążyć wizje żywcem wyjęte z dystopijnego science fiction, jak kontrola umysłów za pomocą fal radiowych czy celowe wywoływanie katastrof naturalnych.

Odporność sieci: dezinformacja w telekomunikacji

Z przeprowadzonych w 2024 roku **badń Eurobarometru** wynika, że Europejczycy czerpią wiedzę o nowych osiągnięciach nauki i technologiach z telewizji (61%), social mediów (31%), prasy – online i papierowej (19%) oraz radia, w tym podcastów (17%). To zrozumiałe, biorąc pod uwagę, że nie każdy jest naukowcem czy pasjonatem nauki wczytującym się w fachowe książki czy periodyki. Niestety oznacza to również, że liczba kanałów nadających się do propagowania nieprawdy jest naprawdę wielka. Szczególnie social media, zachęcające do publikowania własnych treści a jednocześnie generujące bańki informacyjne, świetnie nadają się do rozbudzania niepokoju.

Źródła informacji o rozwoju naukowym i technologicznym



Komu służy dezinformacja?

Podczas zeszłorocznej powodzi pod postem informującym zwolenników teorii spiskowych o rozstawianiu tymczasowego masztu radiowego w Łądku-Zdroju, pojawiło się wiele nienawistnych komentarzy, z których jeden wprost nawoływał do użycia przemocy. Sprawa skończyła się interwencją służb. Droga od podsycania nienawiści do faktycznego przestępstwa jest krótka. Choć ci, którzy rozpowszechniają teorie spiskowe chętnie powołują się na wolność wypowiedzi i potrzebę wyzwolenia się spod jarzma państwa, to sami posługują się skuteczną metodą kontroli społecznej – bo taką jest dezinformacja.

W opublikowanym w styczniu tego roku **raporcie Zespołu ds. Dezinformacji** działającego w ramach powołanej przez rząd Komisji badającej wpływy rosyjskie i białoruskie na bezpieczeństwo wewnętrzne i interesy Rzeczypospolitej w latach 2004-2024 stwierdzono wprost, że rosyjska propaganda aktywnie podsyca teorie spiskowe podważające zaufanie społeczne, w co wpisują się narracje antyszczepionkowe czy anty-5G. Skutkiem działań dezinformacyjnych może być nie tylko doprowadzenie do fizycznego uszkodzenia infrastruktury, ale też zmniejszanie akceptacji społecznej wobec działań niezbędnych dla rozwoju państwa. Kraj, w którym modernizacja i cyfryzacja gospodarki przebiegają wolniej, ma także słabszą pozycję polityczną i jest bardziej narażony na wpływy z zewnątrz.

Odporność sieci: dezinformacja w telekomunikacji

Szukajmy latarni, budujmy zaufanie

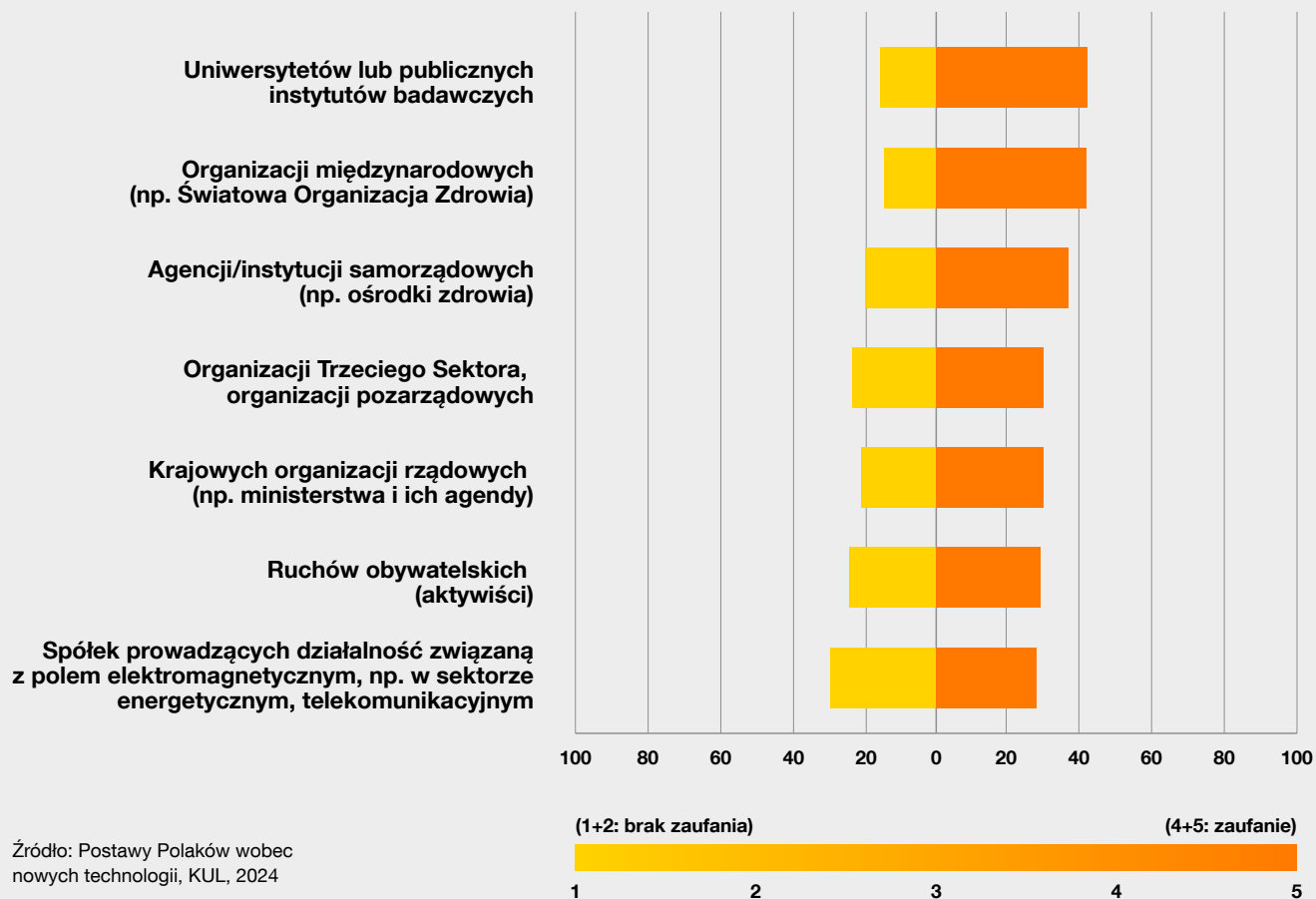
Udzielając odpowiedzi na pytanie jak skutecznie zaradzić dezinformacji na pewno trzeba uwzględnić edukację. Niestety samo skonfrontowanie ludzi z wiedzą naukową nie wystarczy, gdyż od razu pojawiają się pytania: „A widział pan jak robili te badania?”, „A sprawdziła Pani kto opłacał tych naukowców?”.

Zgodnie z powołanymi wcześniej badaniami Eurobarometru, dla aż 54% respondentów z Polski wiedza naukowa nie jest na co dzień przydatna (drugi najwyższy wynik w UE). Co znacznie bardziej szokuje to to, że aż 53% osób stwierdziło, iż naukowcy nie powinni ingerować w debatę publiczną, jeśli decyzje polityczne są niezgodne z dowodami naukowymi. W zakresie tego pytania gorsze wyniki zanotowano tylko na Cyprze, we Włoszech i na Węgrzech.

Ocena samych naukowców jest przy tym niejednoznaczna – z jednej strony zdaniem ankietowanych w Polsce są oni uczciwi (71%), otwarci na dialog z obywatelami (65%) i wiedzą, co jest dla ludzi dobre (64%), ale równocześnie są uważani za ludzi aroganckich (49% – drugi wynik w UE) i o wąskich horyzontach (42% – też drugi wynik w UE). Z kolei z badania prowadzonego przez KUL wynika, że uniwersytety, publiczne instytuty badawcze, organizacje międzynarodowe czy sami naukowcy wciąż cieszą się zaufaniem, choć i w tym zakresie jest spore pole do poprawy.

Zaufanie do instytucjonalnych źródeł informacji

Pytanie: **W jakim stopniu ufa Pan(i) informacjom na temat pola elektromagnetycznego i zdrowia pochodzącym od ...?**
Odpowiadając, proszę posłużyć się skalą od 1 do 5, gdzie „1” oznacza, że w ogóle nie ufa Pan(i) informacjom z tego źródła, a „5”, że ufa Pan(i) całkowicie.



Odporność sieci: dezinformacja w telekomunikacji

Choć wiele zależy od samej polityki państwa, w interesie nas wszystkich jest wskazywanie na wartość, jaką daje nauka. Operatorzy zaangażowani w proces inwestycyjny, tacy jak Orange, z natury rzeczy nie będą postrzegani jako podmioty bezstronne w dyskusji o wpływie technologii na zdrowie czy środowisko.

Nie ma w tym nic złego. Rolą naukowców i niezależnych instytucji jest dokonywanie wiarygodnej oceny w tym zakresie. To, co mogą robić przedsiębiorcy, to wskazywać na wyniki wiarygodnych badań, czy na rzetelne raporty. Warto wyjaśniać także, że nauka rządzi się swoimi zasadami. Z tego, że w dyskursie prezentowane są różne opinie, hipotezy i interpretacje nie wynika jeszcze, że „wszystko ujdzie” i każde zdanie jest tyle samo warte.

Zaufanie nie przychodzi samo. Aby je zyskać potrzeba trudnej i długotrwałej pracy szerokiej koalicji ludzi i organizacji, którym na sercu leżą bezpieczeństwo, rozwój i dobrobyt Polaków. Ten wysiłek jest jednak niezbędny, bo bez zaufania dla wiarygodnych źródeł wiedzy nie uda się zbudować odporności społeczeństwa na dezinformację.



Odporność sieci: powódź



Sławomir Gołygowski
Lider Technologiczny
w Centrum Zarządzania
Usługami
Orange

Wrzesień ubiegłego roku był miesiącem bardzo intensywnej walki z największym kataklizmem ostatnich lat – powodzią w południowo-zachodniej Polsce. Zapewnienie łączności w sytuacji kryzysowej jest kluczowe nie tylko dla skutecznego funkcjonowania służb, ale także dla bezpieczeństwa i spokoju mieszkańców. Robiliśmy więc wszystko, aby zabezpieczyć ciągłość działania naszych usług na terenach dotkniętych powodzią, zapewnić komunikację służbom, a także umożliwić mieszkańcom dostęp do informacji i kontakt z bliskimi.



Trzy województwa: dolnośląskie, opolskie i śląskie zostały objęte stanem klęski żywiołowej i to tam skierowaliśmy największe siły w celu zapewnienia działania naszych obiektów i usług. Na obszarze sześciu kolejnych województw: lubuskiego, wielkopolskiego, łódzkiego, małopolskiego, podkarpackiego i świętokrzyskiego walczyliśmy ze skutkami ulewnych deszczy.

To obszar niemal 160 tys. km², na którym znajdowało się ponad 500 obiektów sieciowych objętych weryfikacją zagrożenia.

W najtrudniejszym momencie 390 z nich nie miało zasilania od dostawców energii. Dzięki wykorzystaniu baterii i agregatów, które dostarczaliśmy wszystkimi możliwymi drogami, także łodziami i samochodami straży pożarnej, większość z nich działała.

Odporność sieci: powódź

Intensywne opady deszczu



9

województw
ok. 160 tys. km²

3

razy/dobę konferencja Sztabu Operacyjnego
wymiana informacji, podejmowanie decyzji

Kontrola stanu wszystkich pomieszczeń
w obiektach sieciowych

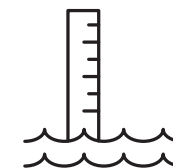
- sprawdziliśmy ponad 500 najważniejszych obiektów sieciowych
- zabezpieczyliśmy infrastrukturę Orange workami z piaskiem i foliami ochronnymi

Wszystkie obiekty krytyczne i strategiczne dla działania sieci Orange zostały zabezpieczone i przez cały ten czas świadczyły usługi telekomunikacyjne.

Premier Krzysztof Gawłowski powiedział, że „w sprawie łączności państwo zdało egzamin”. To stwierdzenie dowodzi, że zaangażowanie zarówno operatorów, jak i administracji przynosi wymierne efekty. Na szczególną uwagę i uznanie zasługują jednak przede wszystkim ci, którzy bezpośrednio w trudnych czy wręcz niebezpiecznych warunkach usuwali powstałe awarie. Służby techniczne Orange i spółki NetWorks błyskawicznie reagowały na każdy zgłoszony przypadek utraconej łączności, starając się jak najszybciej znaleźć optymalne – w tych trudnych okolicznościach – rozwiązania.

W zabezpieczanie infrastruktury Orange oraz w walkę ze skutkami ulewnych deszczów i powodzi zaangażowanych było ponad 250 osób. Zrealizowaliśmy ponad 2000 zadań i przepracowaliśmy 5,5 tysiąca godzin.

Powódź



3

województwa
27 powiatów objętych stanem klęski żywiołowej

70

obiektów
nie świadczyło usług mobilnych w szczytowym momencie akcji (w woj. śląskim, dolnośląskim i opolskim)

33 tys.

zniszczonych
łączy
stacjonarnych

390

obiektów
sieciowych
pozbawionych
zasilania



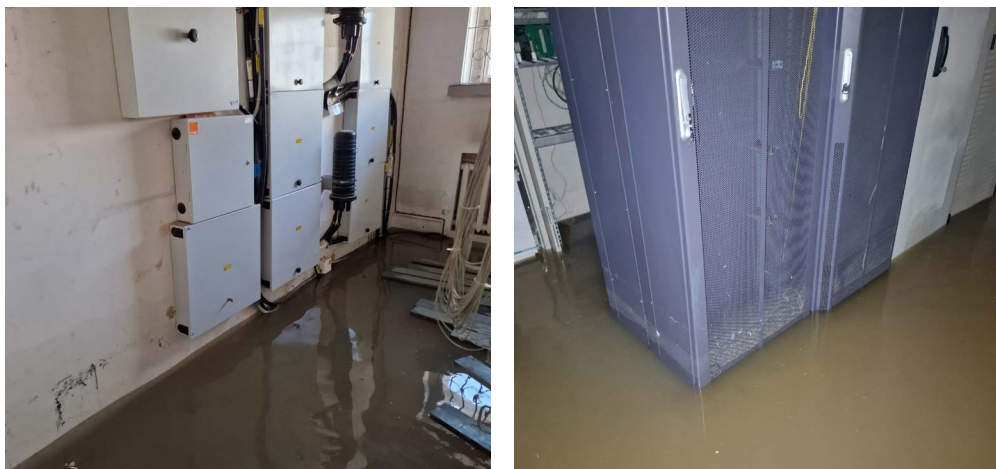
Odporność sieci: powódź

Case study:

Awaria stacji teletransmisyjnej w Lewinie Brzeskim, która służyła do zasilania sygnałem dwóch stacji bazowych w Grodkowie.

Dzięki wyteżonej pracy techników obiekt ten, który w wyniku zalania przestał działać 17 września, odzyskał funkcjonalność już 19. Dzięki przywróceniu zasilania z systemu energetycznego 23. odzyskał pełną sprawność.

Obok przedstawiamy kalendarium usuwania tej awarii.



Informacje te, choć przedstawiają przebieg wydarzeń, nie oddają w pełni skali wyzwania, z którymi musieli mierzyć się pracownicy służb technicznych. Pierwszym krokiem do usunięcia awarii było zdiagnozowanie problemu, co w praktyce wiązało się z koniecznością dostania się do obiektu, który został zalany i znajdował się na terenie, do którego dostęp był co do zasady wyłączony.

Ponieważ warunki nie pozwalały na użycie samochodu, niezbędne stało się skorzystanie z łodzi, a tę należało wypożyczyć. Dzięki pomocy udzielonej w tym zakresie przez Straż Pożarną technicy byli w stanie przypłynąć do obiektu, oszacować straty i przygotować się na jego uruchomienie. W efekcie, po dwóch dniach udało się zastosować tymczasowe rozwiązania służące przywróceniu zasilania.



Wtorek, 17/09

08:14

Zalany obiekt przy ul. Marii Konopnickiej 3 w Lewinie Brzeskim. Zalane i uszkodzone urządzenie teletransmisyjne, które było zainstalowane najniżej w stojaku teletechnicznym.

10:06

Wyłączenie zasilania przez Zakład Energetyczny. Całkowita izolacja węzła, tj. wszystkich urządzeń zainstalowanych w obiekcie.



Środa, 18/09

Brak możliwości dojazdu do obiektu z powodu wysokiego poziomu wody. Realizacja prac przygotowawczych do wymiany zalanego urządzenia oraz tymczasowego zasilania z akumulatorów.



Czwartek, 19/09

10:52

Powrót do nadzoru urządzeń w związku z dostarczeniem do węzła tymczasowych akumulatorów.

15:34

Ponowna izolacja węzła z powodu wyczerpania dostarczonych tymczasowych akumulatorów.

17:39

Powrót do nadzoru urządzeń transmisyjnych w związku z dostarczeniem akumulatorów o większej pojemności.



Piątek, 20/09

14:30-

Prace przy uruchomieniu dostarczonego wcześniej przygotowanego i skonfigurowanego urządzenia teletransmisyjnego.

-15:00

Dostarczenie agregatu prądotwórczego wypożyczonego ze Straży Pożarnej celem doładowywania akumulatorów.



Sobota, 21/09

Dostarczenie na obiekt agregatu prądotwórczego z Orange na potrzeby ładowania akumulatorów.



Poniedziałek, 23/09

Powrót zasilania z Zakładu Energetycznego.

Odporność sieci: klimat



Jan
Gawryszewski
Kierownik Wydziału
Rozwoju Sieci
Orange

Zmiany klimatyczne stanowią poważne zagrożenie dla stabilności i niezawodności sieci telekomunikacyjnej. Ekstremalne zjawiska pogodowe, takie jak huragany, burze, powodzie czy fale upałów, mogą powodować fizyczne uszkodzenia infrastruktury – masztów, wież, kabli oraz stacji bazowych. Zalanie obiektów technicznych czy awarie linii energetycznych prowadzą do przerw w świadczeniu usług.

Problemy te mogą powodować straty finansowe i obniżenie reputacji operatorów, szczególnie gdy awarie są długotrwałe.



Zagrożenia dla ciągłości działania sieci telekomunikacyjnej

Usuwanie skutków powodzi takich jak w 2024 w Kotlinie Kłodzkiej czy innych zalań w obiektach w wyniku nawałnych deszczy absorbuje służby utrzymaniowe, powoduje dodatkowe koszty nadgodzin oraz działań odtworzeniowych na obiektach.

Zmieniające się warunki atmosferyczne mają również wpływ na niezawodność sprzętu telekomunikacyjnego. Silne mrozy i oblodzenie mogą uszkadzać infrastrukturę oraz utrudniać dostęp, co wydłuża czas napraw i konserwacji. Z kolei fale upałów zwiększają ryzyko przegrzewania się sprzętu, prowadząc do awarii.

Systemy klimatyzacyjne projektowane kilkanaście lat temu coraz częściej okazują się niewystarczające dla zapewnienia odpowiednich warunków temperaturowych w pomieszczeniach. Powoduje to ich dodatkową awaryjność, kolejne zaangażowanie służb utrzymaniowych, a w dłuższej perspektywie koszty modernizacji.

Dużym zagrożeniem jest także rosnąca liczba awarii energetycznych spowodowanych ekstremalnymi warunkami pogodowymi po stronie dostawcy energii. Telekomunikacja jest silnie uzależniona od stabilnego zasilania, dlatego przerwy w dostawie energii mogą powodować wyłączenie systemów telekomunikacyjnych. Aby zminimalizować skutki tych zagrożeń inwestujemy w systemy awaryjnego zasilania, takie jak generatory, systemy bateryjne itp.

Efektywność klimatyczna i zużycie energii

Zmiany klimatu mają również istotny wpływ na zużycie energii przez sektor telekomunikacyjny. Wzrost temperatur prowadzi do większego zapotrzebowania na chłodzenie serwerowni, centrów przetwarzania danych oraz pomieszczeń z urządzeniami transmisyjnymi, co znacząco zwiększa koszty operacyjne. Systemy chłodzenia muszą być modernizowane, aby utrzymać stabilne działanie urządzeń i uniknąć przegrzewania infrastruktury, ale także by zwiększyć ich efektywność energetyczną.

Podjęliśmy szereg inicjatyw mających na celu poprawę efektywności energetycznej i zmniejszenie śladu węglowego. Inwestujemy w systemy zasilania gwarantowanego o najwyższej sprawności, aby minimalizować straty energii na jej przetwarzanie, wymieniamy systemy chłodnicze na zużywające mniej energii. Na obiektach pojawiają się panele fotowoltaiczne oraz systemy freecoolingowe. Zastosowanie energooszczędnych rozwiązań pozwala na redukcję kosztów operacyjnych oraz spełnienie wymogów środowiskowych.



Odporność sieci: zagrożenia militarne



Mariusz Ziomek
Główny Architekt
Bezpieczeństwa
Orange



Ewa Jamrozik
Główny Architekt
Bezpieczeństwa
Orange

Czy jesteśmy gotowi na wojnę?

Utrzymywanie ciągłości świadczenia usług telekomunikacyjnych jest wpisane w DNA operatorów. Zarówno na gruncie biznesowym jak i regulacyjnym, operatorzy są zobligowani do utrzymywania sieci na wysokim poziomie dostępności. W Orange, zgodnie z międzynarodowymi standardami, od lat wypracowywane są schematy postępowania w sytuacjach awaryjnych, a każda nowa sytuacja uczy nas jak lepiej i szybciej reagować na pojawiające się zakłócenia działania sieci i usług. Wojna jest jednak sytuacją szczególną.



Gdy 11 lat temu, po przeprowadzeniu kontrowersyjnego referendum, Rosja zaanektowała Krym, a w obwodach Ługańskim i Donieckim rozpoczęła działania zbrojne, niewielu przewidywało, że w niedługim czasie na Starym Kontynencie rozpocznie się pełnoskalowa konwencjonalna wojna. Dopiero napaść Federacji Rosyjskiej na Ukrainę w 2022 roku zburzyła poczucie bezpieczeństwa milionów Europejczyków oraz zachwiała gospodarką europejską.

Najbardziej dotknięty został sektor energetyczny, który stanął w obliczu gwałtownych wzrostów cen surowców i konieczności restrukturyzacji łańcuchów dostaw. Był to zimny prysznic dla wszystkich, którzy uważali, że wojna ich nie dotyczy. W krótkim czasie zarówno firmy państwowe, jak i przedsiębiorstwa prywatne, stanęły przed niełatwym zadaniem dostosowania się do funkcjonowania w nowej rzeczywistości. Wojna niemal w każdej branży wymusiła potrzebę solidnej analizy, często niezbyt aktualnych, strategii bezpieczeństwa oraz dywersyfikację rynków i inwestycje w odporność operacyjną czy cyfrową.

Łączność na wojnie to kluczowy element, który umożliwia koordynację wojsk, przekazywanie rozkazów i informacji wywiadowczych, a także zapewnia komunikację cywilną i międzynarodową. Operatorzy telekomunikacyjni, na których często nakładane są różne zadania związane z bezpieczeństwem narodowym, zaczęli się zatem bacznie przyglądać, z jakimi problemami borykają się ich ukraińscy koledzy i które z tych doświadczeń można już teraz przenieść na własny grunt. Zarówno w kontekście zagrożeń w cyberprzestrzeni, jak i bezpośrednich działań kinetycznych na infrastrukturę.

Odporność sieci: zagrożenia militarne

Zagrożenia militarne, a ciągłość świadczenia usług

Wojna w Ukrainie dobitnie pokazała, jak ważne są komercyjne sieci telekomunikacyjne. Trudno mówić o bezpieczeństwie bez łączności w:

- sektorze energetycznym (komunikacja między elektrowniami, sieciami przesyłowymi i centrami kontrolnymi jest niezbędna do zapewnienia ciągłości dostaw energii i szybkiego reagowania w przypadku awarii),
- transporcie drogowym (zarządzanie ruchem drogowym, kontrolowanie sygnalizacji świetlnej i monitorowanie sytuacji na drogach),
- lotnictwie (koordynacja lotów, zmiany tras, zapobieganie kolizjom) ,
- ratownictwie i sektorze zdrowotnym,
- automatyce przemysłowej,
- zarządzaniu produkcją.

W rzeczywistości wojennej każda utrata obiektu, brak zasilania, czy zniszczenie infrastruktury pociągają za sobą poważniejsze konsekwencje niż w czasie pokoju i są trudniejsze do naprawienia. Ukraińcy mierzyli się przede wszystkim z przerwami w dostawach prądu, fizycznym niszczeniem elementów infrastruktury telekomunikacyjnej, kradzieżami sprzętu, czy odłączaniem użytkowników od ukraińskich dostawców usług na terytoriach okupowanych.

Prawo Komunikacji Elektronicznej

Operatorzy telekomunikacyjni jako podmioty o strategicznym znaczeniu dla funkcjonowania państwa, podlegają licznym regulacjom prawnym, w tym związanym z obronnością i bezpieczeństwem państwa.

Podstawowym aktem normatywnym określającym prawa i obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie komunikacji elektronicznej jest ustawa z 12 lipca 2024 roku, czyli Prawo Komunikacji Elektronicznej, która zastąpiła obowiązujące przez ostatnie 20 lat Prawo telekomunikacyjne.

Celem określonych w tych przepisach obowiązków jest zapewnienie przez przedsiębiorców telekomunikacyjnych ciągłości świadczenia usług telekomunikacyjnych lub dostarczania sieci telekomunikacyjnej poprzez przewidzenie możliwości wystąpienia sytuacji szczególnego zagrożenia. Taką sytuacją jest między innymi zewnętrzne zagrożenie bezpieczeństwa państwa i czas wojny.

Wymaga ona współpracy przedsiębiorców komunikacji elektronicznej z organami administracji publicznej i innymi podmiotami wykonującymi zadania w zakresie ratownictwa, niesienia pomocy, zarządzania kryzysowego, utrzymania porządku publicznego oraz obronności i bezpieczeństwa państwa.



Odporność sieci: zagrożenia militarne

Na takie sytuacje przedsiębiorca telekomunikacyjny powinien posiadać plan działań, obejmujący w szczególności współpracę m.in. z innymi przedsiębiorcami telekomunikacyjnymi (również zagranicznymi) i podmiotami właściwymi w sprawach zarządzania kryzysowego. Plan powinien zawierać cały szereg praktycznych informacji, takich jak:

- środki techniczne i organizacyjne zapewniające poufność,
- integralność, dostępność i autentyczność przetwarzania danych,
- poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka,
- utrzymanie ciągłości dostarczania publicznych sieci telekomunikacyjnych lub świadczenia publiczne dostępnych usług telekomunikacyjnych.



W zależności od rozwoju sytuacji (rozmiaru zagrożenia lub potrzeby ograniczenia jego skutków), Prezes UKE może w sytuacji szczególnego zagrożenia nałożyć na przedsiębiorcę telekomunikacyjnego jeszcze dodatkowe obowiązki, takie jak:

- utrzymanie ciągłości dostarczania publicznych sieci telekomunikacyjnych,
- świadczenie publiczne dostępnych usług telekomunikacyjnych,
- ich odtwarzanie z uwzględnieniem pierwszeństwa dla operatorów usług kluczowych i operatorów infrastruktury krytycznej,
- ograniczenie:
 - zakresu lub obszaru eksploatacji publicznych sieci telekomunikacyjnych i urządzeń telekomunikacyjnych,
 - świadczenia niektórych publicznie dostępnych usług telekomunikacyjnych,
 - używania urządzeń radiowych.

Ważne dla skuteczności planu jest, aby był on aktualny, uzgodniony z interesariuszami oraz wprowadzony do stosowania w organizacji.

System Bezpiecznej Łączności Państwowej

Doświadczenia wojenne naszych sąsiadów oraz nasze własne w trakcie pokoju (np. podczas powodzi), pokazują, że brakuje w Polsce systemu łączności dedykowanej administracji państwowej. Dlatego w długo wyczekiwanej Ustawie o ochronie ludności i obronie cywilnej, pojawił się zapis o stworzeniu Systemu Bezpiecznej Łączności Państwowej.



SBŁP to wielowarstwowy system składający się ze zbioru zastępowalnych elementów powiązanych ze sobą relacjami w taki sposób, że stanowią one całość. W założeniach w skład SBŁP będą wchodzić podsystemy:

- łączności stacjonarnej (jawnej i niejawnej),
- wielopunktowej wideokonferencji,
- bezpiecznej radiowej łączności mobilnej, w tym niejawnej komórkowej,
- bezpiecznej radiowej łączności trankingowej,
- bezpiecznej łączności satelitarnej, w tym niejawnej.

Aktualnie trwają prace nad przygotowaniem szczegółowych wymagań dla tego systemu.



Ustawa o obronie Ojczyzny

Wojna na Ukrainie przyczyniła się też do przyspieszenia procesu legislacyjnego związanego z wejściem w życie Ustawy o obronie Ojczyzny, konsolidującej regulacje występujące w kilkunastu innych ustawach oraz kompleksowo przebudowującej system obronny naszego kraju.

Jej poprzednia oraz wielokrotnie aktualizowana wersja, obowiązywała od 1967 roku i zupełnie nie odpowiadała współczesnym potrzebom. Przepisy ustawy regulują kwestie związane z realizacją zadań przez przedsiębiorców na rzecz sił zbrojnych, którzy mogą być zobowiązani do:

- produkcji, dostaw lub świadczenia usług na rzecz wojska w czasie kryzysu lub wojny,
- przygotowania zasobów np. transport, magazyny, systemy teleinformatyczne na potrzeby obronne,
- wykonania świadczeń rzeczowych polegających na przekazaniu lub udostępnieniu posiadanych nieruchomości i rzeczy ruchomych do używania przez Siły Zbrojne.

Tym samym każdy operator telekomunikacyjny (jak każdy inny przedsiębiorca), na którego nałożono obowiązek realizacji zadań na rzecz Sił Zbrojnych, jest zobligowany do ich realizacji na podstawie stosownej decyzji administracyjnej, zgodnie z określonymi dla danego zadania warunkami i zakresem.

Dodatkowo operatorzy telekomunikacyjni zwykle stanowią element programowania obronnego, w ramach którego przygotowywane są plany operacyjne zawierające szczegółowe wytyczne w zakresie współpracy z administracją rządową w celu zapewnienia bezpieczeństwa i ciągłości funkcjonowania kraju.

Programowanie obronne obejmuje szereg działań, które umożliwiają pełne wykorzystanie zasobów państwowych i prywatnych w celu zapewnienia gotowości obronnej państwa w każdym możliwym scenariuszu. I pomimo, że w obecnym porządku prawnym nie funkcjonuje już ustawa o przedsiębiorcach o szczególnym znaczeniu gospodarczo-obronnym, która wprost z nazwy wskazywała poszczególne firmy, to należy się spodziewać, że największe przedsiębiorstwa telekomunikacyjne zostaną włączone do systemu organizacji zadań obronnych w naszym kraju.

Oczywiście jakość przygotowania obronnego, realizacji zadań na rzecz Sił Zbrojnych, czy też zapewniania potrzeb w zakresie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa, będzie zależała od rzetelności oraz jakości działań przygotowujących do realizacji tych zadań, czy samego ich zdefiniowania. Być może właśnie zmiana przepisów w tym obszarze oraz wynikające z nich nowe dokumenty planistyczne i realnie określone potrzeby, stanowiąc będą o jakości przygotowania przedsiębiorców do realizacji zadań na rzecz bezpieczeństwa państwa. Zapewne potwierdzenia tej tezy należy się spodziewać w niedalekiej przyszłości, w związku choćby z terminami określonymi w obowiązujących przepisach a dotyczącymi ważności dotychczasowych decyzji administracyjnych, czy zawartych umów.

Pozostałe regulacje

Mówiąc o bezpieczeństwie państwa i jego obywateli nie sposób nie wspomnieć o innych regulacjach, które nakładają na licznych przedsiębiorców dodatkowe obowiązki w tym obszarze. W pierwszej kolejności mowa o infrastrukturze krytycznej, pełniącej kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli. Infrastruktura krytyczna to w myśl definicji zawartej w ustawie o zarządzaniu kryzysowym, systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania administracji publicznej, a także instytucji i przedsiębiorców. Dla tego typu obiektów przedsiębiorcy będący operatorami infrastruktury krytycznej, zobligowani są do przygotowania planów ochrony, ostatecznie zatwierdzanych przez Rządowe Centrum Bezpieczeństwa.

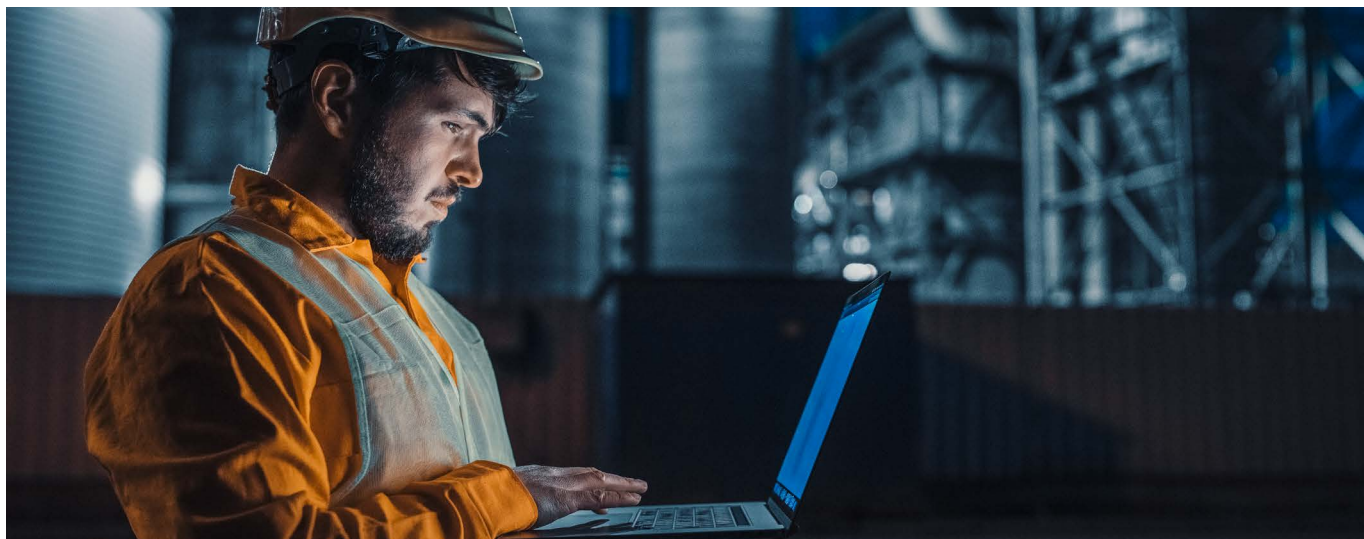
Obok infrastruktury krytycznej w prawie polskim obowiązuje także termin obowiązkowej ochrony, która również dotyczy obszarów, obiektów, urządzeń i transportów ważnych dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych istotnych interesów państwa. Ustawa o ochronie osób i mienia, która określa obiekty podlegające obowiązkowej ochronie oraz sposób ich zabezpieczenia i ochrony, również nakłada szereg obowiązków na właścicieli takich obiektów (a jak nietrudno się domyślić, główni operatorzy telekomunikacyjni dostarczający usługi łączności, choćby na potrzeby służb ratowniczych, znajdują się w tej grupie).

Niestety mnogość przepisów oraz brak odpowiedniej synchronizacji między nimi często prowadzą do sytuacji, w której zamiast koncentrować się na rzeczywistej ochronie obiektów, skupiamy się na formalnościach, które nie zawsze przyczyniają się do zwiększenia bezpieczeństwa, a w wielu przypadkach mogą wręcz powodować rozproszenie zasobów i nieefektywność w zarządzaniu bezpieczeństwem.

Jako operatorzy telekomunikacyjni nie dysponujemy środkami obrony infrastruktury przed atakiem rakietowym czy ostrzałem artyleryjskim. Procedury odtwarzania infrastruktury bez względu na przyczynę jej zniszczenia (mogą to być np. zjawiska pogodowe), wyglądają podobnie. Różnica oczywiście polega na utrudnionym dostępie do danego obszaru, który może być objęty strefą wojny, brakiem kadry zdolnej do wykonywania prac serwisowych na terenie bezpośredniego zagrożenia, czy problemami z utrzymaniem łańcucha dostaw.

Epilog

Wszystkie obecnie obowiązujące, jak i te procedowane regulacje prawne (dyrektywy unijne NIS2, CER, które będą transponowane do prawa krajowego), przyczyniają się do zwiększenia odporności na różnego typu zagrożenia. Stanowią one również istotny element w zwalczaniu zagrożeń charakterystycznych dla wojny hybrydowej, w której jako narzędzia walki wykorzystywane są ataki cybernetyczne, w szczególności ukierunkowane na zakłócenie ciągłości funkcjonowania infrastruktury krytycznej, intensywne działania w przestrzeni informacyjnej, szerzenie propagandy, dezinformacji oraz manipulacji opinią publiczną. W prawodawstwie związanym z szeroko pojętym bezpieczeństwem wiele się jednak zmieniło na dobre i wiele się jeszcze zmieni.



4 Okiem liderów rynku

Opinie i analizy dotyczące rynku telekomunikacyjnego:

- Telko.in
- Fiberhost
- Nexera
- Światłowód Inwestycje





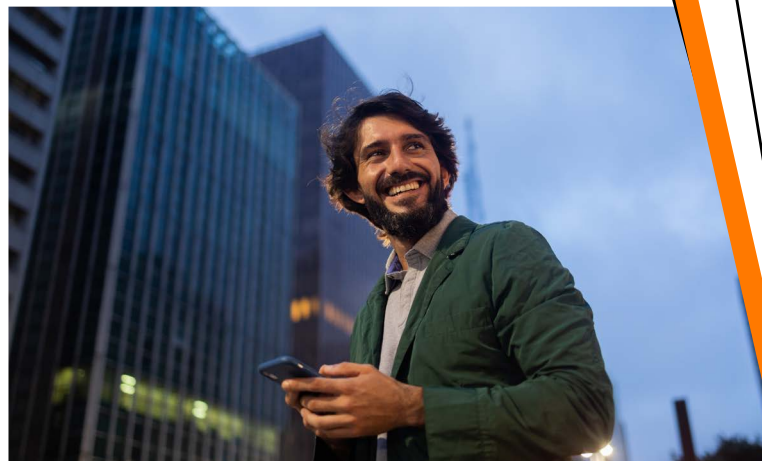
Wartość rynku usług międzyoperatorskich, na którym – na dobrą sprawę – ściśle komercyjnie działa tylko jeden operator, łatwo umyka rynkowym statystykom. Niemniej można co nieco wycisnąć z tego, co publikuje regulator rynku oraz poszczególni gracze na tym rynku.

„Ponad 900 mln zł” – to kwota określająca wartość rynku hurtowego, jaka pada w ostatnim raporcie o stanie rynku telekomunikacyjnego Urzędu Komunikacji Elektronicznej za rok 2023. Licząc dokładnie, wartość ta wyniosła 941 mln zł. W skonsolidowanym raporcie Orange za 2024 ror czytamy natomiast o przeszło 1,6 mld zł z całego segmentu hurtowego operatora. Niespójne? Nieporównywalne? Zgadza się. Z całego rynku hurtowego raport UKE uwzględnia tylko udostępnianie lokalnych pętli abonenckich w modelu BSA i LLU oraz udostępnianie linii WLR. Raport Orange tymczasem uwzględnia wszystkie linie produktowe pionu hurtu, w tym (przede wszystkim) terminację połączeń w sieciach mobilnych i stacjonarnych.

Przyjrzyjmy się (w miarę możliwości) poszczególnym nisząom rynku hurtowego, do którego – wedle metodyki raportowej Orange – należą: **„przychody od operatorów telekomunikacyjnych z tytułu usług komórkowych: połączenia przychodzące od innych operatorów, usługi roamingu dla osób odwiedzających, krajowe połączenia komórkowe (tj. umowa roamingu krajowego i udostępniania sieci), udostępnianie infrastruktury komórkowej i MVNO, usług stacjonarnych i udostępniania infrastruktury stacjonarnej, oraz inne przychody (głównie transmisja danych).”**

Optyczny dostęp na topie

Hurtowe usługi na infrastrukturze dostępowej, to rosnący segment rynku. Bazując na raportach UKE, można powiedzieć, że w latach 2022-2023 (świeże dane dostępne będą dopiero w lipcu) urosł wartościowo o 15% tj. o blisko 100 mln zł. Jest to oczywiście tylko i wyłącznie zasługa BSA w sieciach optycznych.



Raport UKE co prawda nie rozróżnia poszczególnych technologii, ale z danych publikowanych przez Orange widać wyraźnie spadek liczby usług BSA na sieci miedzianej oraz głosowych usług WLR.

Wzrost wartości rynku optycznego dostępu potwierdzają także jednostkowe dane operatorów hurtowych. Wartość przychodów Światłowodu Inwestycji wzrosła w 2024 roku do 297 mln zł (204 mln zł w 2023), a wartość przychodów Nexery do 120 mln zł (87 mln zł w 2023). Przychody Polskiego Światłowodu Otwartego wyniosły 653 mln zł, a wzrost (można tylko szacować, ponieważ dane za 2023 rok nie są porównywalne) ok. 11 proc. Fiberhost raportu za 2024 rok jeszcze nie opublikował, a Tauron Obsługa Klienta nie wyróżnia w sprawozdaniach finansowych działalności na niedawno zbudowanej sieci optycznej. Podobnie Orange Polska, ale w przypadku tego operatora dostępne są operacyjne dane o sprzedaży optycznych linii hurtowych. Na koniec 2024 roku udostępniał ich 156 tys., co oznacza roczny wzrost o 39 tys., za czym powinien być pójść wzrost (a co najmniej utrzymanie) przychodów.



Nieubłagany jest natomiast rynek dla usług w sieci miedzianej. Na koniec 2024 roku pozostało 148 tys. linii WLR oraz 56 tys. linii BSA. Jeden i drugi rynek kurczy się w tempie kilku tysięcy linii kwartalnie. Te dane dotyczą tylko sieci Orange Polska, ale ten operator na nim dominuje. Z danych UKE za 2023 rok wynika, że obsługiwał 93% wszystkich linii WLR. Rynek ten wart był w 2023 90 mln zł, co oznaczało spadek o 16%. Co do wartości, to 62% przypadało na abonentów indywidualnych a reszta na firmy. Oba segmenty te kurczą się zresztą w podobnym tempie.

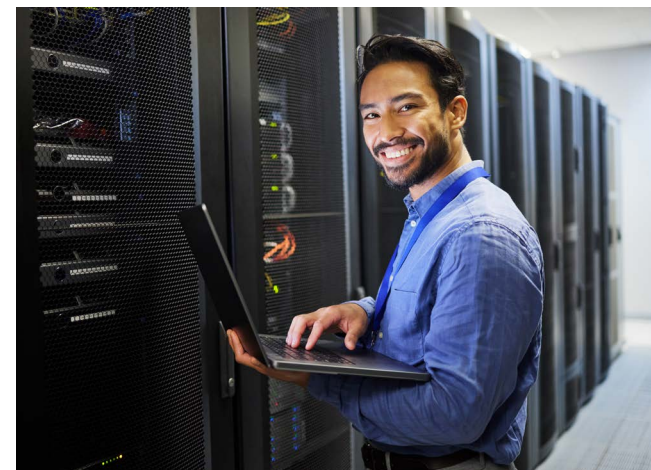
Dla BSA w sieci miedzianej brak danych, ponieważ statystyki UKE nie wyróżniają segmentów xDSL i FTTH. Aktywnych usług BSA FTTH jest jednak o dwa rzędy wielkości więcej, a więc przychody z usług miedzianych mogą stanowić tylko niewielką frakcję całego rynku BSA i to z tendencją malejącą.

Istnieje jeszcze ponadto „nisza nisz”, czyli usługi świadczone poprzez uwolnione lokalne pętle miedziane (LLU). Na koniec ubiegłego roku Orange raportował już tylko 22 tys. użytkowników takich linii, wobec 29 tys. rok wcześniej. Tymczasem raport UKE mówi o 59 tys. linii LLU na koniec 2023 roku i 31,5 mln zł przychodów z tego rynku – o 2% mniej, niż w 2022.

Terminacja połączeń pod presją

Hurtowy rynek głosowy znajduje się pod silną presją spadku jednostkowych stawek FTR/MTR, co wynika z unijnych regulacji. O ile jednak wartość rynku MTR „wypłukuje” tylko erozja stawek, o tyle rynek FTR zarówno erozja stawek, jak korzystanie z usług i liczby klientów.

Na mobilnym rynku głosowym w 2023 roku UKE raportuje łącznie wydzwonienie przez abonentów 111 mld minut przy wartości rynku przekraczającym 15 mld zł. Wartość tego rynku uwzględnia abonamenty, ale wobec popularności taryf nielimitowanych trudno jest odnieść wolumen ruchu do całkowitego przychodu. Poza planami nielimitowanymi w 2023 roku staryfikowano połączenia o wartości ponad 2,4 mld zł. Rok wcześniej wolumen ruchu był o 4 mld minut większy, ale całkowite przychody o 900 mln zł wyższe. Wartość połączeń poza planami nielimitowanymi bardzo nieznacznie wzrosła.



Na tle rynku detalicznego można przeanalizować dane z rynku hurtowego, które pod względem wolumenu ruchu...prawie się nie zmieniły. Inaczej z przychodami (1,781 mld zł). Wartość rozpoczętych połączeń głosowych spadła o 31%. a wartość terminacji o 16%. Tylko tranzyt w sieciach mobilnych urósł o 8%. Nie zmienia to faktu, że cały rynek mobilnego interkonektu spadł w 2023 o 13%. Nie mamy jeszcze zbiorczych danych dla 2024 roku, ale przychody Orange z hurtu mobilnego skurczyły się w tym okresie o 14%.

Jeżeli chodzi o rynek stacjonarny, to jako całość (usługi detaliczne) miał w 2023 roku wartość 924 mln zł przy wolumenie 2,4 mld minut. Rok do roku wolumen połączeń zmniejszył się o 650 mln minut, a wartość o 146 mln zł. Adekwatnie do tego rynek interkonektowy (227 mln zł) skurczył się o 14%.

W roku 2024 – w przypadku Orange Polska – spadek wyniósł 4% – sporo mniej niż cały rynek. Nie wiemy, czy najświeższe wyniki Orange wskazują na spowolnienie spadku, czy poszły wbrew trendom całego rynku, czy też może – co wydaje się najbardziej prawdopodobnym – niepełną spójnością danych, jakie podaje UKE i operator. Tym bardziej, że w ubiegłym roku Orange dokonał reklasyfikacji usług i do przychodów z MTR/FTR zaczął doliczać przychody z usług infrastrukturalnych na sieciach – odpowiednio – mobilnych i stacjonarnych.

Roaming i MVNO

Spadek stawek jednostkowych dotyczy także specyficznego rynku roamingu dla abonentów sieci zagranicznych. W 2023 roku jego wartość przekroczyła 360 mln zł, co oznaczało 4% spadek.

Ten spadek zaistniał przy jednoczesnym znaczącym wzroście wolumenu obsługiwanej mobilnej transmisji danych, niewielkim wzroście liczby połączeń roamingowych oraz spadku liczby SMS.

Pewne ożywienie zapanowało w ciągu ostatnich trzech lat na rynku MVNO, a więc i jemu warto poświęcić uwagę. Ożywienie to dotyczy bardziej enablerów, którzy liczą na współpracę detalicznych partnerów, niż abonentów gotowych korzystać z SIM pod alternatywnymi markami.

Jak podaje UKE, na koniec 2023 roku na rynku funkcjonowało 139 operatorów mobilnych świadczących usługi w sieci jednego z dużych MNO. Rok wcześniej takich przedsiębiorców było 122, a więc zainteresowanie działalnością MVNO rośnie. Inaczej z zainteresowaniem klientów, którzy w marginalnym stopniu interesują się usługami operatorów alternatywnych. W 2021 roku MVNO obsługiwali 4,1% wszystkich kart SIM, rok później 3,5%, a na koniec 2023 – 3,1%. Ich udział w przychodach spadł z 2,4 do 2,1%. To, co prawda, oznacza niebagatelną kwotę 321 mln zł, ale główny udział w tym torcie mają operatorzy infrastrukturalni obsługujący połączenia. Dla MVNO pozostaje niewiele.

Trzeba nadmienić, że w 2022 roku Virgin Mobile połączył się z P4 i wniósł do Play swoją bazę kliencką, co znacznie uszczupliło stan posiadania MVNO w rynku. Nie widać jednak podmiotów, które miałyby potencjał, aby wypełnić powstałą lukę.



Cenna infrastruktura

Gdyby ze segmentu hurtowego wyłączyć dostęp szerokopasmowy oraz terminację połączeń głosowych, to pozostanie przede wszystkim klasyczny rynek udostępniania infrastruktury. Na ten temat jednak nie ma już żadnych zbiorczych danych. Bazować można tylko na raportach Orange (i ewentualnie innych graczy). Unikalną szansę dała zeszłoroczna reklasyfikacja przychodów w pionie hurtu Orange. Do dotychczas raportowanych przychodów z terminacji mobilnej i stacjonarnej operator dołożył przychody z udostępniania właściwej infrastruktury. Na tej podstawie można szacować, że udostępnianie infrastruktury mobilnej przynosiło mu w 2023 roku 45 mln zł, a infrastruktury stacjonarnej – 290 mln zł.

Jeżeli chodzi o infrastrukturę mobilną, to odnośnikiem dla wyników Orange mogą być wyniki spółek z grupy Cellnex Poland. OnTower, spółka konsolidująca dawne aktywa sieciowe Play, zanotowała 729 mln zł przychodów (+13%). Zysk operacyjny wyniósł 66 mln zł. Przychody Towerlink, które jest dysponentem i obsługuje infrastrukturę sieci Plus, wyniosły 1,453 mld zł (+13%) przy 251 mln zł zysku operacyjnego. Warto pamiętać, że Towerlink kupił i obsługuje także aktywne urządzenia, gdy OnTower tylko wieże i maszty. Waloryzacja cen dzierżawy infrastruktury wpisana jest w ramowe porozumienia pomiędzy Towerlink/OnTower a operatorami sieci.

Pośród infrastrukturalnych graczy można jeszcze wymienić Emitel, który dysponuje 700 obiektami telekomunikacyjnymi różnej wysokości. W 2023 roku przychody operatora z dzierżawy miejsca na tych obiektach wyniosły 97 mln zł i wzrosły o 16%.



Sytuacja i model biznesowy wymienionych wyżej podmiotów jest inny, co utrudnia analizę całego rynku. Ponieważ jednak zasoby telekomunikacyjne w Polsce rosną, to uzasadnia wzrosty przychodów dysponentów infrastruktury pasywnej.

I jeszcze transmisja

Na koniec można wspomnieć rynek transmisji danych, który może niekoniecznie ma charakter ściśle hurtowy, chociaż z pewnością stanowi część oferty międzyoperatorskiej. Po reklasyfikacjach przychodów hurtowych dokonanych przez Orange Polska odnaleźć go można w pozycji „Pozostałe usługi hurtowe”.

Ich wartość na koniec ubiegłego roku wyniosła 159 mln zł – o 7 mln zł więcej, niż 2023. Na potrzeby tych usług operator rozbudował pojemność sieci transmisyjnej z 19,9 Tb/s do 24,7 Tb/s na koniec 2024 roku (uruchomił także pierwszy kanał optyczny 800G).

Wzrost przychodów z transmisji raportuje także Emitel – w 2023 (raportu za zeszły rok jeszcze brak) wyniosły 22 mln zł – nieznacznie więcej, niż rok wcześniej.

Niezmienne regulacje i zmieniający się rynek – perspektywy i wyzwania rynku hurtowego



Tomasz Zmyślony
Strategic Business
Unit Director
Fiberhost

Krok ku przyszłości – co czeka rynek w 2025 roku?

Możemy się spodziewać dalszego wzrostu dostępu do sieci FTTH w Polsce. W dużej mierze będzie to wynikało z inwestycji operatorów mających infrastrukturę miedzianą, którzy nakładają na nią sieć światłowodową (S-I, PŚO, Fiberhost). Według raportu PMR Market Experts "Rynek telekomunikacyjny w Polsce 2024. Analiza rynku i prognozy rozwoju na lata 2024-2029" technologia światłowodowa stanowi już obecnie ponad połowę wszystkich łączy dostępowych w Polsce¹ i ten współczynnik będzie w kolejnych latach rósł.

Sukcesywnie zmienia się też chęć operatorów do dzielenia się informacjami ewidencyjnymi na temat swojej infrastruktury. I nie chodzi tutaj o obowiązki sprawozdawcze, ale dobrowolne dzielenie się danymi, które jeszcze kilka lat temu uznawane były za wrażliwe. Przykładem może być aplikacja „GeoGrid” Fiberhost.

Dzięki niej współpracujący z nami Operator Korzystający ma dostęp do różnych warstw infrastruktury oraz może wyznaczyć odległość od interesującego go punktu do najbliższego punktu elastyczności sieci Fiberhost. Narzędzie znacząco powinno ułatwić podłączanie klientów biznesowych i zwiększyć wykorzystanie istniejącej już sieci.

Otwartość rynku na dzielenie się wiedzą, szukanie nowych pomysłów na rozwój i ogromne inwestycje realizowane przez



operatorów to bez wątpienia dobra wiadomość. Szkoda, że podobnego podejścia nie widać wśród administratorów systemu SIDUSIS, gdzie dostęp do danych jest bardzo ograniczony.

Gorsza informacja jest taka, że za ogromnymi pieniędzmi, które stoją za budową nowej infrastruktury nie idzie proporcjonalny wzrost wartości rynku telekomunikacyjnego w Polsce. Według corocznych raportów UKE wartość rynku między 2018 a 2023 wzrosła o 3,3 mld zł (z 39,7 do 43,0 mld), przy skumulowanych nakładach inwestycyjnych (Capex) w tym czasie wynoszących 60,6 mld zł. Inwestycje te były głównie skierowane na rozwój infrastruktury światłowodowej, modernizację sieci oraz przygotowania do wdrożenia technologii 5G. Oczywiście na zwrot w infrastrukturę trzeba czasami czekać kilkanaście albo kilkadziesiąt lat, jednak trudno oprzeć się wrażeniu, że rynek w Polsce rozwija się wolno.

¹) https://pl.investing.com/news/stock-market-news/pmr-wartosc-ryнку-telekomunikacyjnego-wzrosła-o-2-rr-do-56-mld-zł-w-2024-roku-802536?utm_source=chatgpt.com

Niezmienne regulacje i zmieniający się rynek – perspektywy i wyzwania rynku hurtowego

Tu warto dodać, że w 2025 i kolejnych latach powinniśmy obserwować znaczącą zmianę w strukturze inwestycji – z budowy stacjonarnych sieci światłowodowych na upgrade sieci mobilnych do 5G, a z czasem do 6G. Przyczyni się to znacząco do poprawy bezprzewodowego dostępu do internetu, jak również rozwoju inteligentnych miast oraz Internetu Rzeczy (IoT).

W przypadku infrastruktury światłowodowej w oczu rzucają się dwa główne wyzwania. Pierwsze z nich to zauważalna, malejąca dynamika zapotrzebowania na usługi FTTH. Wynika to w dużej mierze z problemów demograficznych, w tym starzejącego się społeczeństwa i stosunkowo niskich kompetencji cyfrowych, z którymi boryka się Polska.

Przełamanie tego impasu możliwe jest tylko przy ścisłej współpracy operatorów hurtowych i detalicznych. Wspólne działania komunikacyjne i edukacyjne powinny kłaść nacisk na użyteczność technologii.

W drugiej kolejności należy wymienić zbyt niskie ceny internetu, jedne z najniższych w całej Europie. To oczywiście dobrze dla klienta końcowego, źle dla operatorów i prowadzonych przez nich inwestycji. Warto jednak dodać, że Polska nie jest tutaj wyjątkiem w Europie. Według raportu „State of Digital Communications 2024” cały nasz region ma znacząco mniejsze ARPU z usług telekomunikacyjnych niż USA, Korea Południowa, Chiny czy Japonia².

W bieżącym roku będziemy też obserwować coraz odważniejsze próby wykorzystywania AI w biznesie telekomunikacyjnym.

Technologia pomoże operatorom zarówno w optymalizacji sieci i zarządzaniu infrastrukturą, jak i automatyzacji procesów. Na pewno przełoży się to na rozwój nowych usług a także obsługę klienta i doświadczenie użytkownika. Operator, który pierwszy będzie w stanie wdrożyć i skutecznie korzystać z możliwości sztucznej inteligencji będzie w stanie, przynajmniej krótkoterminowo, zyskać przewagę konkurencyjną.

Ostatnim zjawiskiem, które warto będzie obserwować na rynku polskim jest konsolidacja a raczej jej brak. Rynek polski jest bardzo rozdrobniony i nic nie wskazuje na to, żeby w najbliższych latach miało się to zmienić.

Także w 2025 nie widać na horyzoncie spektakularnych fuzji. To jest też bolączka całego rynku europejskiego. W Europie jest 45 dużych grup operatorów, którzy mają ponad 500 tys. klientów, w porównaniu z 8 w USA, 4 w Chinach i Japonii oraz 3 w Korei Południowej. W konsekwencji spada zdolność inwestycyjna całego sektora i możliwość konkurowania z gigantami z Azji i USA.

Rok 2025 zapowiada się więc jako rok stabilnego, choć powolnego wzrostu. Pozostaje mieć nadzieję, że niestabilne otoczenie regulacyjne stanie się bardziej przewidywalne i prorozwojowe, niż do tej pory.



2) <https://connecteurope.org/>

Rynek światłowodowy w Polsce dojrzał i wciąż ma przed sobą ogromny potencjał



Paweł Biarda
Członek Zarządu
ds. komercyjnych
NEXERA

Dynamiczny rozwój sieci światłowodowych w ostatnich latach wraz z pojawieniem się operatorów hurtowych i multi-swiatłowodu sprawił, że polski rynek telekomunikacyjny należy dziś ocenić jako dojrzały. Obecnie nawet 60% internautów w Polsce korzysta ze światłowodu¹, co nadal pozostawia duży potencjał do wzrostu – zarówno w rozszerzaniu zasięgów jak i wypełnieniu sieci usługami. Wyzwaniem dla operatorów hurtowych pozostaje dotarcie do jak największej liczby użytkowników internetu z przesłaniem o korzyściach płynących z multi-swiatłowodu.

W obszarze cyfryzacji Polska wykonała w ostatnich latach ogromny krok naprzód. Dostęp do szerokopasmowego internetu ma obecnie niemal 7,7 mln z niewiele ponad 9 mln punktów adresowych, a nasz kraj plasuje się dziś powyżej średniej unijnej pod względem zasięgu sieci światłowodowych i infrastruktury o bardzo wysokiej przepustowości. Ważny wpływ na zwiększenie dostępu do szerokopasmowych łączy miał także dynamiczny rozwój rynku hurtowego.

Multi-swiatłowód systematycznie zwiększa swój zasięg w kraju, choć nie doczekał się dużej publicznej kampanii promocyjnej, tak jak choćby technologia 5G. Dziś mówimy już o milionach użytkowników. W kolejnych latach w zasięgu operatorów hurtowych znajdą się dalsze obszary, które nie mają jeszcze dostępu do multi-swiatłowodu.



Dostępność łącza światłowodowego dla wielu dostawców detalicznych istotnie zmieniła obraz rynku w ostatnich latach. Również z punktu widzenia odbiorcy końcowego, ponieważ daje możliwość wyboru z ofert wielu operatorów. Jest to możliwe, ponieważ multi-swiatłowód działa w modelu „jeden kabel – wiele usług”. Dzięki temu, konsumenci mogą dowolnie wybierać między najlepszymi dla nich pakietami dostawców internetu, telewizji, usług VoD czy telefonii VoIP oraz zmieniać ich bez konieczności wymiany łącza.

¹) Raport Regiony Nexery 2024 „Polacy w internecie – rozrywka, praca, codzienność”

Rynek światłowodowy w Polsce dojrzał i wciąż ma przed sobą ogromny potencjał

Obecnie, w zasięgu multi-światłowodu Nexery znajduje się ponad 750 tys. gospodarstw domowych w 5,8 tys. miejscowościach, w siedmiu województwach. Jednak zapewnienie zasięgu to tylko połowa sukcesu. Ważną kwestią wciąż pozostaje szybkie pozyskanie dużej liczby użytkowników, czyli skuteczna komercjalizacja istniejącej już infrastruktury. W tym zakresie aż się prosi o wsparcie żmudnych i kosztownych działań promocyjnych realizowanych przez operatorów komercyjnych, działaniami prowadzonymi przez administrację państwową. Korzystanie ze światłowodu jako strategicznego medium komunikacji w Europie powinno być promowane jak najszerzej i w każdy możliwy sposób.



W Polsce wciąż istnieje ponad 2,4 mln gospodarstw domowych bez dostępu do szybkiego internetu (tzw. białe plamy NGA). Jest to istotna szansa na dalszy rozwój dla całego rynku hurtowego dostępu do sieci. Dlatego, w strategii Nexery na najbliższe lata, zakładamy dalsze rozszerzanie zasięgu naszego multi-światłowodu i osiągnięcie poziomu ponad 1,5 miliona gospodarstw domowych. Inni operatorzy hurtowi mają równie ambitne plany. Żeby je zrealizować wszyscy potrzebujemy ułatwień w dostępie do danych o infrastrukturze już istniejącej. Także uproszczenie procedur administracyjnych będzie dużym ułatwieniem. Pozwoli to możliwie dobrze planować i realizować inwestycje.

Bardzo ważne dla dalszego rozwoju rynku internetu światłowodowego i modelu hurtowego będzie otwarta współpraca hurtowników z detalistami nad stałym podnoszeniem liczby użytkowników multi-światłowodu. Synchronizacja działań komercyjnych, w tym trade-marketingowych, przekazywanie informacji o zasięgach oraz skuteczności sprzedaży, które zapoczątkowaliśmy jako Nexera na polskim rynku przyjęło się na dobre i dziś jest to stały element współpracy wszystkich dużych hurtowników i detalistów działających na ich sieciach. W najbliższym czasie będziemy też obserwować rosnącą rolę innowacyjnych rozwiązań sprzedażowych, dostosowanych do specyfiki mniejszych miejscowości i bardziej dojrzałych sieci, co w Nexerze mamy już na porządku dziennym. Wierzymy, że w tym zakresie dużo jeszcze da się zrobić tak, by wszyscy będący w zasięgu stali się też użytkownikami multi-światłowodu.



Rozwój Rynku Infrastruktury Telekomunikacyjnej: perspektywa Światłowodów Inwestycje



Magdalena Russyan
COO
Światłowodów Inwestycje

Telekomunikacja odgrywa kluczową rolę w dzisiejszym zglobalizowanym świecie, cyfryzacja i rozwój infrastruktury telekomunikacyjnej, zwłaszcza sieci światłowodowych, staje się priorytetem dla wielu krajów. W Polsce, jednym z liderów tego rozwoju jest firma Światłowodów Inwestycje – uznanie zyskaliśmy dzięki dynamicznym inwestycjom i wybitnym wynikom.

Możemy poszczycić się ponad 2 milionami gospodarstw domowych w zasięgu swojej sieci, z czego prawie 1,5 miliona zostało przyłączonych w latach 2021-2024. To tempo inwestycji stawia nas w czołówce operatorów sieci światłowodowych w Polsce. W ciągu ostatnich trzech lat liczba aktywnych usług wzrosła o ponad 280%, osiągając obecnie ponad 600 tysięcy. Co więcej, osiągamy 92% skuteczności dostarczania usług.

Inwestujemy nie tylko w rozwój technologiczny, ale kładziemy też duży nacisk na zrównoważony rozwój. Nasz przygotowany w 2024 roku Raport Zrównoważonego Rozwoju za rok 2023 nagrodzony został za debiut, co świadczy o naszym zaangażowaniu w kwestie ekologiczne i społeczne. W 2024 roku rozpoczęliśmy korzystanie ze zrównoważonego finansowania, tzw. Green Loan, co dodatkowo podkreśla naszą dbałość o środowisko. Dotychczas wydaliśmy już ponad 2,9 miliarda złotych na budowę sieci światłowodowej.



Zasięg naszej sieci obejmuje **ponad 2 mln** gospodarstw domowych



Pracowity rok za nami – wybudowaliśmy sieć dla 400 tys. gospodarstw domowych



Nasz internet światłowodowy jest już w ponad **600 tys.** mieszkań w Polsce



W zeszłym roku uruchomiliśmy usługi **215 tys.** klientom



Jesteśmy eko – zaczęliśmy korzystać ze zrównoważonego finansowania **Green Loan**

Rozwój Rynku Infrastruktury Telekomunikacyjnej: perspektywa Światłowodów Inwestycje



Sieć

- Ponad 2 mln gospodarstw domowych w zasięgu sieci Światłowodów Inwestycje
- 1,5 mln gospodarstw domowych zasięg wybudowany w latach 2021-2024



Klienci

- Ponad 600 tys. aktywnych usług (wzrost o ponad 280% w ciągu 3 lat)
- 92% skuteczności dostarczania usług
- Niezawodność – 99,97% rocznej dostępności usługi (czasu ciągłego działania usługi)



ESG

- Raport Zrównoważonego Rozwoju nagroda za debiut w 2023 roku
- Badanie GRESB (Global Real Estate Sustainability Benchmark) 94/100 pkt w badaniu, wysoki wynik, powyżej średniej
- Green Loan w 2024 zaczęliśmy korzystać ze zrównoważonego finansowania



Finanse

- 2,5 mld zł nakładów na budowę sieci FTTH i przyłączy klienckich w ciągu 3 lat
- 670 mln zł przychodów ze strzaży usług w ciągu 3 lat

Z naszej perspektywy, rozwój infrastruktury światłowodowej w Polsce ma przed sobą świetlaną przyszłość. Szanse rozwoju rynku są ogromne, szczególnie w kontekście rosnącego zapotrzebowania na szybki i niezawodny internet. Operatorzy hurtowi odgrywają kluczową rolę w zapewnianiu dostępu do nowoczesnych technologii dla szerokiego grona odbiorców. Jednakże, branża telekomunikacyjna stoi również przed pewnymi zagrożeniami.

Wyzwania związane z wysokimi kosztami inwestycji, rosnącymi oczekiwaniami klientów oraz regulacjami prawnymi mogą wpływać na dynamikę rynku. Dlatego też, firmy muszą być elastyczne i innowacyjne, aby sprostać tym wyzwaniom i nadal rozwijać swoje usługi.

Technologiczne innowacje

Jednym z najważniejszych czynników wpływających na rozwój branży telekomunikacyjnej jest postęp technologiczny. Operatorzy na sieciach światłowodowych rozpoczynają przygotowania do wdrożenia technologii XG-PON będącej następcą używanej obecnie technologii GPON. Technologia XG-PON umożliwia oferowanie na istniejącej infrastrukturze światłowodowej usług do 10 Gb/s.

XG-PON to przyszłość internetu w Polsce, ale pełnoskalowe wdrożenie wymaga kilku lat, dlatego operatorzy będą wprowadzać tę technologię stopniowo. Pomimo to, w najbliższych latach możemy spodziewać się coraz szerszej dostępności usług abonenckich do 10 Gb/s. Jednocześnie rośnie popularność technologii mobilnych, głównie 5G.

Struktura rynku

Struktura rynku telekomunikacyjnego w Polsce jest zróżnicowana i obejmuje zarówno dużych operatorów, jak i mniejsze firmy. Dominujący udział na rynku mają wiodący operatorzy, którzy oferują pełen zakres usług, od telekomunikacji stacjonarnej i mobilnej po szerokopasmowy dostęp do internetu i usługi telewizyjne.

W 2023 roku światłowod dostarczany przez operatorów hurtowych sięgał już ponad 17 tys. miejscowości, czyli o ponad 1,5 tys. więcej niż w roku poprzednim. Pod względem liczby miejscowości objętych zasięgiem sieci operatora hurtowego pierwsze miejsce należało do Fiberhost (9,7 tys.). 5 tys. miejscowości objęła zasięgiem Nexera. Światłowod Inwestycje dotarł do 1,4 tys. Zwiększyła się także liczba budynków podłączonych do otwartych sieci szerokopasmowych, których w 2023 było ponad 2,3 mln. Najwięcej z nich obejmował swoją działalnością Fiberhost (905,8 tys.). W 2023 roku zwiększyła się także liczba gospodarstw domowych korzystających ze światłowodu.

Operatorzy hurtowi odnotowali skokową poprawę wyników, a największe zasięgi zaraportowały Światłowod Inwestycje (1,7 mln) oraz Polski Światłowod Otwarty (3,7 mln) z zastrzeżeniem, że w przypadku Polskiego Światłowodu Otwartego ponad 3 mln gospodarstw domowych jest zrealizowane co najmniej częściowo w technologii HFC (koncentrycznej). (Raport o stanie rynku telekomunikacyjnego w 2023 roku, str. 92-93).

Trendy konsumenckie

Zmieniające się potrzeby i oczekiwania konsumentów są kolejnym kluczowym czynnikiem kształtującym rynek. Użytkownicy coraz częściej oczekują wysokiej jakości usług, elastycznych pakietów oraz konkurencyjnych cen. Wzrost popularności usług streamingowych, gier online oraz telepracy wymusza na operatorach ciągłe dostosowywanie oferty i infrastruktury. Operatorzy muszą być elastyczni i innowacyjni, aby sprostać wymaganiom rynku oraz utrzymać swoją konkurencyjność.

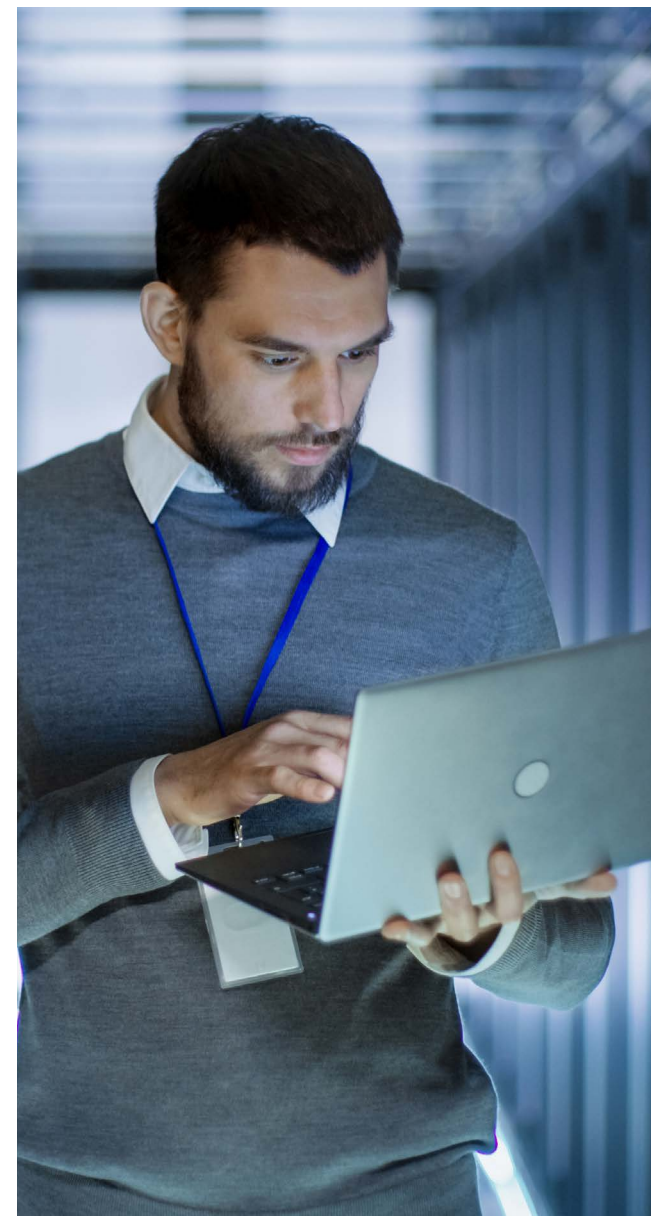
Konsolidacja rynku telekomunikacyjnego w latach 2023-2024

Obserwujemy znaczący wzrost liczby przejęć operatorów z segmentu SME przez większych operatorów oraz fundusze inwestycyjne. Przyspieszenie tego trendu zwiastuje także pojawienie się inwestora finansowego w postaci funduszu Arcus w FIXMAPie, który do tej pory przejął około 20 operatorów i dysponuje zasięgiem 270 tys. gospodarstw domowych, a według doniesień prasowych planuje znaczące przyspieszenie kolejnych akwizycji, będąc w procesie negocjacji z nawet 20 kolejnymi podmiotami.

Proces konsolidacji jest napędzany przez rosnące koszty prowadzenia działalności telekomunikacyjnej, konieczność modernizacji sieci do wyższych przepływności oraz presję na wysoką jakość usług ze strony klientów. Jednocześnie usługi telekomunikacyjne w Polsce pozostają jednymi z najtańszych w Europie.

Prognozy rozwoju

Prognozy na lata 2023-2028 wskazują na stabilny wzrost branży telekomunikacyjnej w Polsce. Oczekuje się, że rynek będzie się rozwijał zarówno pod względem wartości, jak i zasięgu usług. Według szacunków firmy PMR Market Experts, wartość rynku telekomunikacyjnego w Polsce wyniosła w 2024 roku 56 miliardów złotych, co stanowi wzrost o 2% w porównaniu z 2023 rokiem. Pomimo wyzwań, takich jak wysokie koszty inwestycji i rosnące oczekiwania konsumentów, branża telekomunikacyjna w Polsce ma ogromny potencjał do dalszego rozwoju. Istotnym elementem będą przejęcia i konsolidacja rynku.



5 Technologie i komunikacja

- Automatyzacja sieci optycznych
- Światłowodowe systemy czujnikowe
- Copper Switch Off
- Przewagi technologii mobilnych



Trendy w sieciach optycznych i ich rola w ewolucji rynku



Adam Grodecki
Product Line
Manager
Nokia

2024 był rokiem ciągłego odkrywania nowych, efektywniejszych modeli działania i rozwoju biznesu, pozwalających na redukcję kosztów i przyspieszenie wzrostu przychodów. Strategie skupiały się na obszarach uproszczenia, bezpieczeństwa, cyfryzacji i automatyzacji sieci transportowych, ze szczególnym uwzględnieniem eksploracji sztucznej inteligencji w kontekście sieci autonomicznych. W tym artykule podsumujemy trendy rynkowe w sieciach optycznych, rosnące obawy związane z zagrożeniami kwantowymi i ich wpływem na sieci, a także spojrzymy na rozwój sieci pozaziemskich.

W 2024 roku automatyzacja w sieciach optycznych nabrała rozpędu

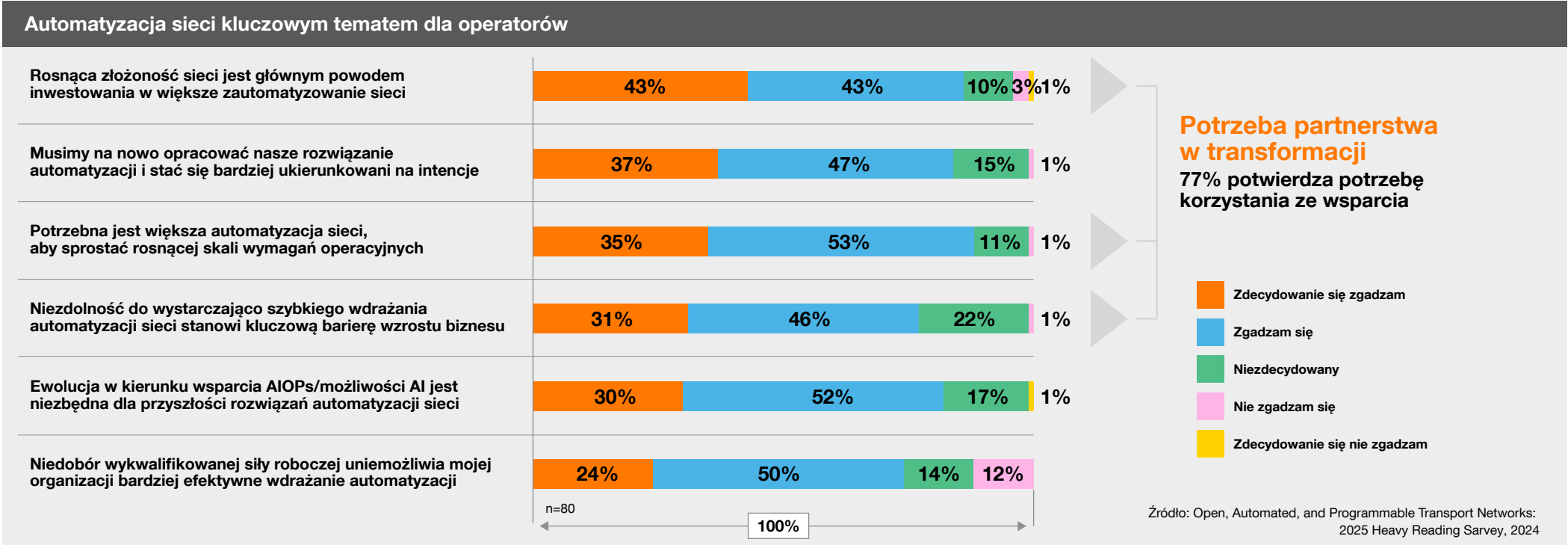
Automatyzacja sieci optycznych, napędzana była w 2024 roku przez postępy w dziedzinie sztucznej inteligencji, otwartych architektur oraz konwergencji sieci IP i optycznych. Kluczową przeszkodą na drodze do jej upowszechnienia pozostają jednak wyzwania związane z koordynacją między domenami.

Wraz z rosnącą liczbą nowych funkcji technologicznych i aplikacji zaprojektowanych do wspierania projektowania, planowania, udostępniania, zapewniania i optymalizacji sieci, rośnie złożoność integracji skalowania. Wyzwanie ułatwiają pojawiające się i ewoluujące standardy branżowe za pośrednictwem interfejsów API, a także przyjęcie automatyzacji sieci w pętli zamkniętej w celu digitalizacji istniejącego procesu operacyjnego.

Zgodnie z wynikami ankiety Heavy Reading Survey dotyczącej otwartych, zautomatyzowanych i programowalnych sieci transportowych, wdrażanie automatyzacji jest kluczowe dla operatorów. W większości przypadków barierą dla adopcji jest jednak możliwość wprowadzenia takiej automatyzacji na tyle szybko, aby sprostać wyzwaniom organizacyjnym i technicznym. W takim przypadku warto skorzystać ze wsparcia doradczego lub projektowego profesjonalnych usług dostawców sieci, którzy mogą mieć lepszy wgląd w technologie i szybciej wprowadzić takie rozwiązania automatyzacji. W efekcie przyspieszyć realizację celów biznesowych i skrócić czas wprowadzania produktów na rynek.



Trendy w sieciach optycznych i ich rola w ewolucji rynku



Konsultacje z dostawcami sieci coraz częściej stają się praktyką w zapewnieniu płynnej integracji ze starszymi systemami i zapewniają operatorom sieci możliwość ograniczenia ryzyka operacyjnego.

W przypadku złożonych wdrożeń (np. transformacji węzłów optycznych) dostawcy sieci uznali za konieczne zwrócenie się o specjalistyczną wiedzę i wsparcie do praktyk serwisowych dostawców sieci. Takie podejście zmniejsza ryzyko związane z dostawcami sieci i zapewnia większą elastyczność we wdrażaniu systemów transportowych, które są zgodne z ich wymaganiami biznesowymi dotyczącymi obszarów miejskich lub regionów.

Potwierdza to raport Omdia „Telco Network and Service Automation Market Tracker Report – 2024”, w którym podkreślono, że ponad 70% operatorów telekomunikacyjnych wprowadza rozwiązania automatyzacyjne w ramach istniejącej infrastruktury, we współpracy z dostawcami sieci. Strategia ta przyspiesza wdrażanie automatyzacji, minimalizując jednocześnie zakłócenia. Współpraca z dostawcami umożliwia także efektywne skalowanie narzędzi automatyzacji w różnych warstwach sieci, zwiększając efektywność operacyjną i upraszczając wyzwania integracyjne w zmieniającym się otoczeniu rynkowym.

Przykładem możliwości takiego narzędzia, które pozwala operatorom na kontrolę, optymalizację

i skalowanie wydajności sieci jest platforma WaveSuite wdrożona w ramach operatorskiej sieci optycznej. Badanie ilościowe przeprowadzone przez Analysys Mason i Nokię dotyczące automatyzacji sieci optycznych z wykorzystaniem WaveSuite wskazało na znaczne oszczędności kosztów operatorów telekomunikacyjnych:

- zmniejszenie o 56% kosztów operacyjnych zarządzania cyklem życia sieci,
- o 26% zmniejszone nakłady inwestycyjne,
- przewidywany wzrost przychodów o 10%, dzięki poprawie konkurencyjności,
- skrócenie średniego czasu realizacji zleceń serwisowych z 10 dni do 24 godzin.

Trendy w sieciach optycznych i ich rola w ewolucji rynku

2024 był kolejnym rokiem udanych wdrożeń terenowych, pokazujących korzyści operacyjne i postęp w automatyzacji sieci optycznych. Udoskonalenia, jakie Nokia wprowadziła na platformie WaveSuite dotyczą m.in. zwiększonej przepustowości, niezawodności i niskich opóźnień. Obejmują integrację systemów wsparcia biznesowego (BSS) z funkcjami sieci optycznej, która obsługuje technologię Network-as-a-Service (NaaS) w celu wdrażania i realizacji poziomu usług warstwy 1.

Automatyzacja sieci optycznych wykracza jednak poza oprogramowanie i aplikacje. Pozwala także na przekształcanie modeli operacyjnych, transformację biznesową i polepszanie bezpieczeństwa sieci. Ponad 77% ankietowanych operatorów korzysta z pomocy dostawców w zakresie automatyzacji, a ponad 40% wprowadziło nowe modele operacyjne i transformacyjne.

W 2024 roku automatyzacja umożliwiła aktualizacje oprogramowania przy znacznie niższym ryzyku (KPI na poziomie 99,1%) i na znacznie większą skalę (87% aktualizacji zostało zautomatyzowanych). Dzięki tym ulepszeniom ponad 40% klientów firmy Nokia może przeprowadzać aktualizacje oprogramowania sieciowego w ciągu dnia, co ułatwia płynne wdrażanie poprawek i udoskonalień. To ważne rozwiązanie wzmacniające odporność sieci optycznej.

Ubiegłoroczne, ciągłe ewolucje automatyzacji sieci podkreśliły również znaczenie praktyk bezpieczeństwa w ochronie systemów zarządzania sieciami z myślą o bezpieczeństwie wbudowanym w platformy, jednocześnie podkreślając znaczenie certyfikatów bezpieczeństwa w celu poprawy tolerancji ryzyka wobec cyberataków.

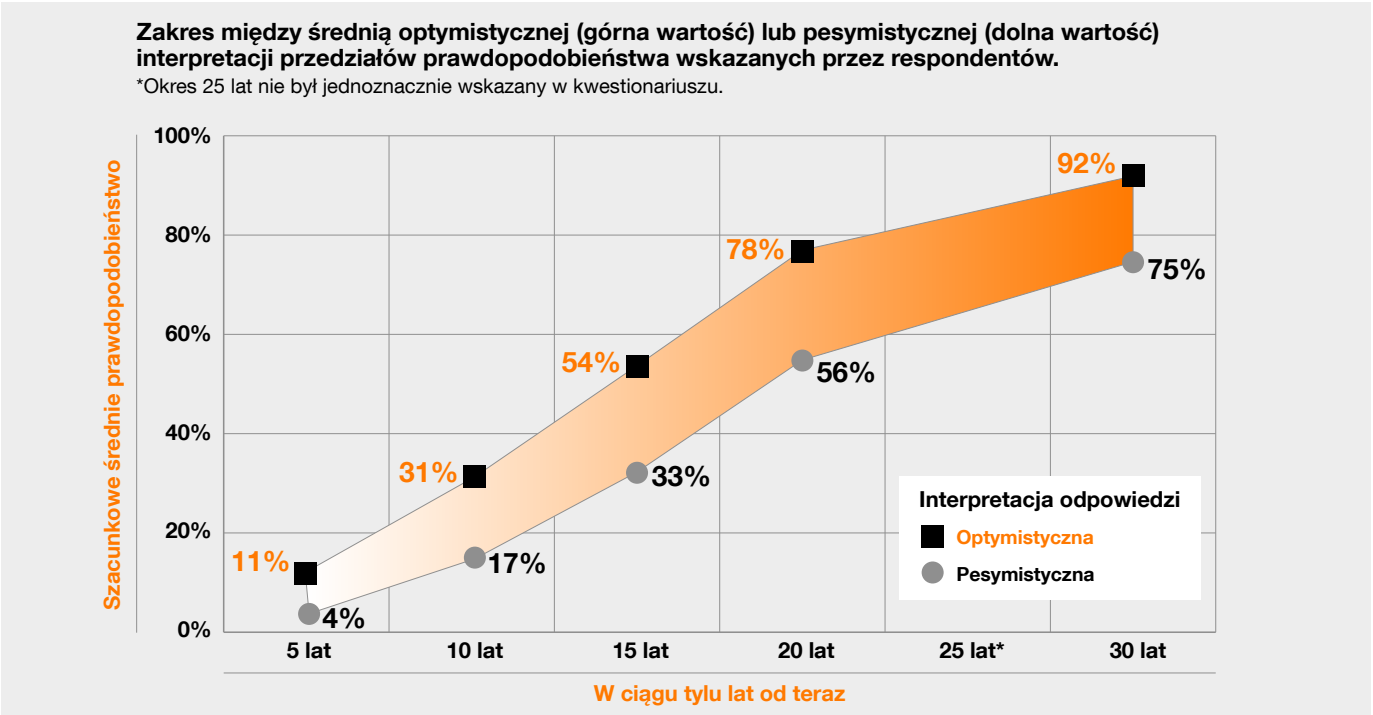
Uzupełnieniem tych praktyk jest również rozwijanie cyberbezpieczeństwa w zakresie ochrony przed zagrożeniami fundamentalnymi dla przyszłości cyberbezpieczeństwa – sieciami Quantum Safe.

Sieci kwantowo bezpieczne: zabezpieczenie cyfrowej przyszłości

W 2024 roku rynki światowe były bardziej wyczulone na nadchodzące zagrożenie ze strony komputerów kwantowych posiadających możliwości odszyfrowania algorytmów kryptograficznych opartych na matematyce. Pojawienie się komputerów kwantowych, wykorzystujących kubity zdolne do istnienia w wielu stanach jednocześnie (a nie tylko

w stanach dwubiegunowych 1 i 0, jak w naszej obecnej cyfrowej taksonomii), zrewolucjonizuje dziedziny takie jak zrównoważony rozwój, obrona, medycyna i finanse. Jednak ich zdolność do łamania istniejących protokołów szyfrowania budzi poważne obawy dotyczące bezpieczeństwa danych.

Problem ten pogłębiają strategię „zbierz teraz, odszyfruj później”, zgodnie z którymi zebrane dziś zaszyfrowane dane, czekają, aż uda się je odszyfrować, gdy możliwości kwantowe osiągną dojrzałość. Oś czasu jest już przewidziana w jednym z przykładów przedstawionych w raporcie Quantum Threat Timeline Report Global Risk Institute – Executive Summary (styczeń 2024).



Trendy w sieciach optycznych i ich rola w ewolucji rynku

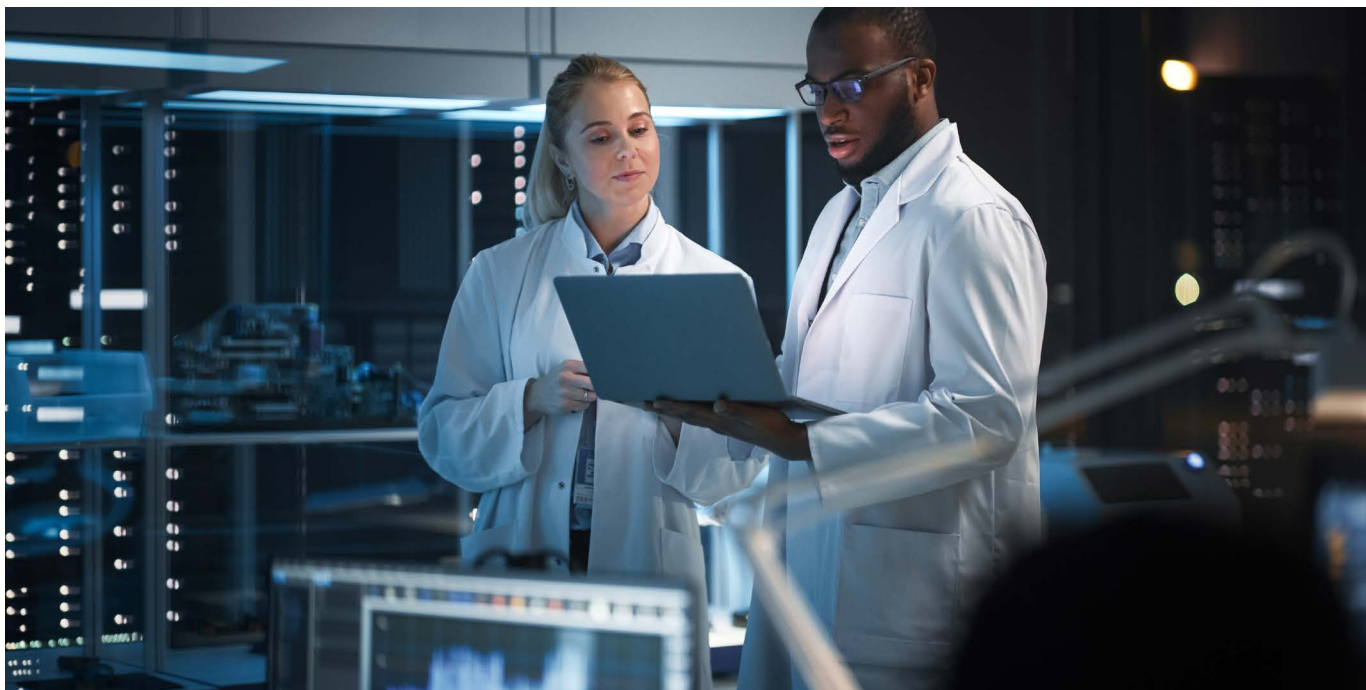
Standaryzacja i rozwój polityki

Wysiłki normalizacyjne wspierają przejście na środki bezpieczeństwa odporne na kwanty. Amerykański Narodowy Instytut Standardów i Technologii (NIST) zatwierdził nowe algorytmy kryptografii postkwantowej (PQC), co stanowi znaczący krok w kierunku ustanowienia solidnych, kwantowo bezpiecznych standardów algorytmów kryptograficznych. Środki te są niezbędne, aby zastąpić obecne, słabe algorytmy infrastruktury klucza publicznego (PKI), powszechnie stosowane w wielu aplikacjach wykorzystywanych w infrastrukturze krytycznej, w tym w sieciach energetycznych, systemach finansowych i sieciach opieki zdrowotnej.

Aby zapewnić sieci przyszłościowe, liderzy branży i instytucje badawcze aktywnie opracowują rozwiązania bezpieczne kwantowo, które można zintegrować z istniejącą infrastrukturą. Opracowywany jest m.in. projekt naziemnych i podwodnych sieci IP oraz optycznych sieci kwantowo-bezpiecznych. Wczesne próby przeprowadzone w 2024 r. odegrały kluczową rolę w przygotowaniu gruntu pod ekosystem cyfrowy zabezpieczony kwantowo.

Reakcja przemysłu i innowacje

Dostrzegając te wyzwania, istnieje pilna potrzeba opracowania rozwiązań, które mogą spełnić zasady MOSQA niezbędne do ocen ryzyka przed zagrożeniami cyberbezpieczeństwa oraz rozwoju bezpiecznych sieci kwantowych. Zasady MOSQA stanowią miarę osi czasu, w którym dane w systemach komunikacyjnych muszą pozostać zabezpieczone, wraz z czasem potrzebnym na



modernizację takich systemów, aby mogły być odporne na kryptograficznie istotne ataki oparte na komputerach kwantowych. Działania te muszą zostać podjęte, zanim te komputery kwantowe zostaną uruchomione z wystarczającą mocą, aby złamać wykorzystywaną kryptografię. Jeśli oś czasu jest zbyt długa, ryzyko jest zbyt wysokie, a dane mogą być naruszone. Ta zasada pomaga d[ostawcom] usług zrozumieć, jak niebezpieczne mogą być komputery kwantowe i jak ważny jest czas niezbędny do aktualizacji systemów, aby zapobiegać tego typu naruszeniom. Wiodące organizacje, w tym Nokia, przodują w rozwoju sieci Quantum Safe. Sieci te integrują klasyczne i kwantowe metody generowania kluczy, aby zapewnić niezawodne szyfrowanie na

różnych poziomach połączeń, zapewniając dogłębną ochronę, odporność kryptograficzną i umożliwiając płynne przejście na wyższy poziom bezpieczeństwa.

Nokia stosuje proaktywne i prewencyjne podejście do promowania elastyczności kryptograficznej w warstwach aplikacji. Promuje wykorzystanie algorytmów kryptografii postkwantowej (PQC, np. z NIST) do ochrony kwantowej, ponieważ aplikacje te zazwyczaj wykorzystują infrastrukturę klucza publicznego (PKI) przy użyciu asymetrycznej wymiany kluczy ze względu na ogromną liczbę aplikacji na całym świecie oraz skalę i szybkość, z jaką można je przyjąć w takim systemie.

Trendy w sieciach optycznych i ich rola w ewolucji rynku

Te algorytmy kryptograficzne, wraz z symetryczną dystrybucją kluczy używanymi w warstwach IP i transportowych, tworzą zwinną i odporną sieć kryptograficzną. Podejście do symetrycznej dystrybucji kluczy jest stosowane w tych warstwach, ponieważ mają one o rzędy wielkości mniej połączeń w porównaniu z tymi w warstwach aplikacji.

Podejście bezpieczne kwantowo wykorzystuje:

- klucze współdzielone,
- symetryczną dystrybucję kluczy,
- źródło klucza o wysokiej entropii (oparte na fizyce kwantowej lub klasycznej),
- techniki szyfrowania z dużą szybkością, takie jak Advanced Encryption Standard (256-bitowy AES).

Współpraca firmy Nokia z HellasQCI w Grecji pokazała, że podejście hybrydowe jest możliwe. Polega ono na dystrybucji kluczy Quantum Safe (fizyki klasycznej i kwantowej) w infrastrukturze krytycznej w trzech lokalizacjach w Grecji. Podkreśla to kluczową rolę odporności kwantowej, gdy generowanie kluczy pochodzi z sieci kwantowej dystrybucji kluczy (QKD).

Rosnące zapotrzebowanie na prywatność i bezpieczeństwo danych doprowadziło do udoskonalenia algorytmów szyfrowania – w tym sztucznej inteligencji i zaawansowanych technik matematycznych - w celu wzmocnienia obrony przed przyszłymi kwantowymi atakami kryptograficznymi. Co więcej, technologie kwantowe wykazują obiecujące postępy w skutecznym zabezpieczeniu zasobów cyfrowych, wykrywaniu zagrożeń i komunikacji, wykorzystując takie techniki jak splątanie kwantowe i QKD. Nad takimi technikami komunikacji pracują także uczelnie w Polsce.

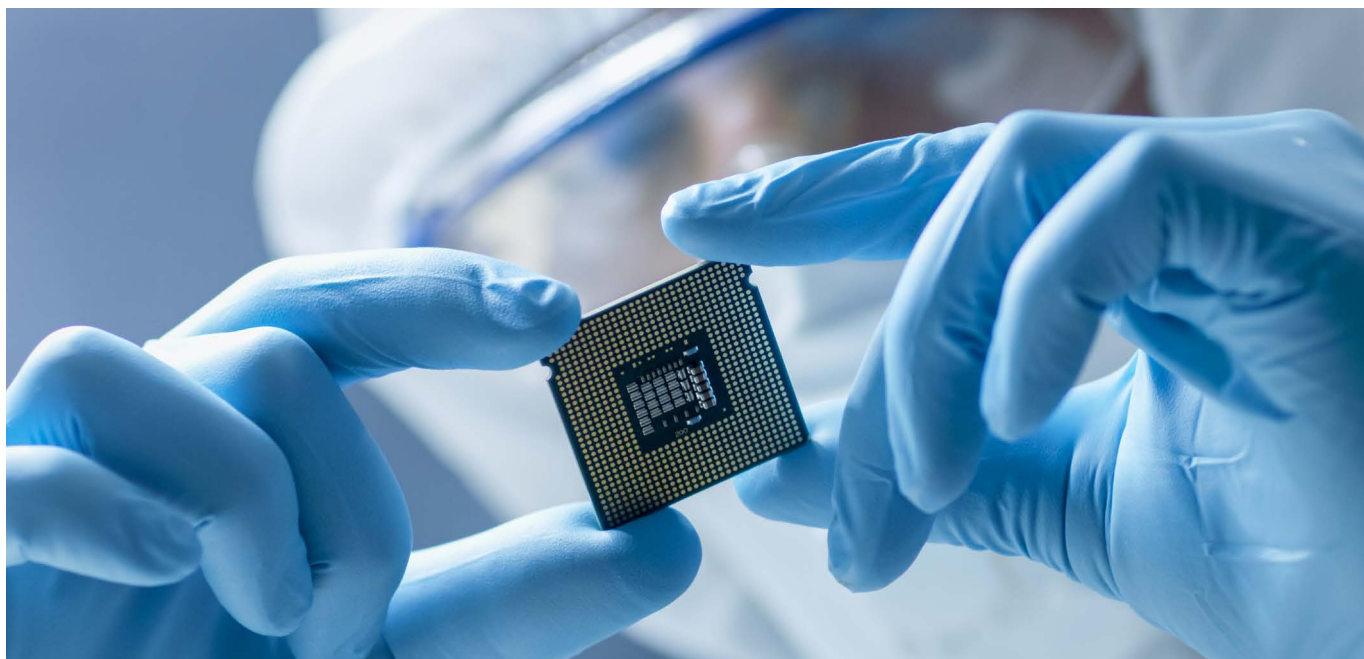
Przygotowanie do ery kwantowej

Zbliżające się pojawienie istotnych kryptograficznie komputerów kwantowych (CRQC) przyspieszyło wysiłki na rzecz oceny zależności kryptograficznych i wdrożenia rozwiązań bezpiecznych kwantowo. Transformacja ta jest nie tylko ulepszeniem technologicznym, ale fundamentalną zmianą niezbędną do zapewnienia integralności i prywatności danych w erze kwantowej.

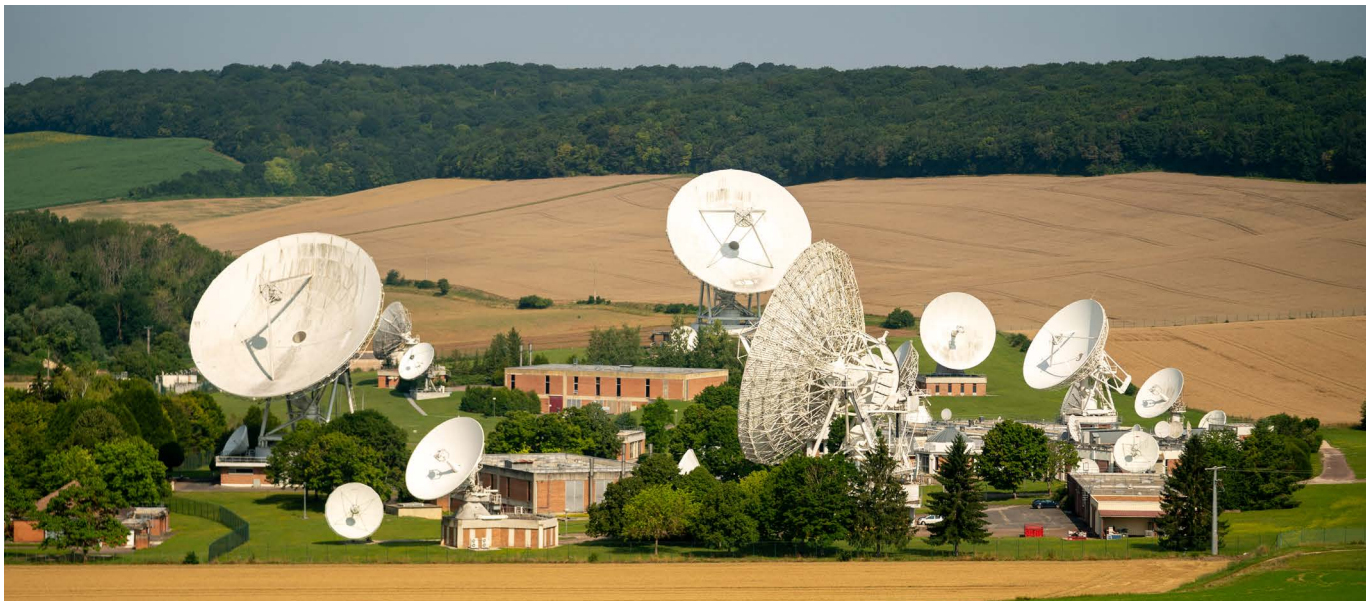
Matematycy, fizycy i kryptolodzy aktywnie rozwijają postkwantowe algorytmy kryptograficzne zaprojektowane tak, aby wytrzymać potencjalne ataki kwantowe. Ponadto nowe metody kwantowej dystrybucji kluczy są integrowane z klasycznymi sieciami, umożliwiając generowanie kluczy wstępnych

i automatyzację w celu zwiększenia bezpieczeństwa. Postępy te umożliwiają współistnienie kryptografii bezpiecznej kwantowo z infrastrukturą klucza publicznego (PKI) oraz istniejącymi zaszyfrowanymi strukturami danych.

Globalna reakcja dotycząca potencjalnego wpływu obliczeń kwantowych na cyberbezpieczeństwo doprowadziła do znacznych postępów w rozwoju sieci bezpiecznych kwantowo. Ogólnobranżowa współpraca między podmiotami komercyjnymi i środowiskami naukowymi zapewnia, że infrastruktura cyfrowa pozostaje odporna na potencjalne zagrożenia kwantowe. W miarę udoskonalania technik kryptograficznych i integracji QKD z tradycyjnymi systemami, kładzie się podwaliny pod bezpieczną kwantowo ekonomię.



Trendy w sieciach optycznych i ich rola w ewolucji rynku



Sieci pozaziemskie są oparte na laserach: rok 2024 kształtuje przyszłość komunikacji kosmicznej

W szybko rozwijającej się dziedzinie komunikacji satelitarnej, zwrot w kierunku sieci optycznych zrewolucjonizuje sposób przesyłania danych poza atmosferę ziemską. Rosnące zapotrzebowanie na szybką, bezpieczną i wolną od zakłóceń komunikację przyspieszyło już przyjęcie technologii laserowego cyfrowego przetwarzania sygnału, wykorzystującą (DSP) transceiver. To początek nowej ery, w której sieci kosmiczne opierają się głównie na laserach, a nie na tradycyjnych częstotliwościach radiowych. Główni gracze to NASA, Airbus, Thales i Mitsubishi Electric.

Wzrost popularności optycznego procesora DSP w kosmosie

Laserowe systemy komunikacyjne oferują niezrównane korzyści w porównaniu z konwencjonalnymi systemami opartymi o częstotliwości radiowe (RF). Należą do nich wyższe szybkości transmisji danych, zmniejszone opóźnienia i odporność na zakłócenia elektromagnetyczne. Optyczny procesor DSP pozwala na precyzyjne przetwarzanie sygnału, umożliwiając wydajną i niezawodną transmisję danych na ogromne odległości, w tym misje międzyplanetarne i eksplorację głębokiego kosmosu.

Pokaz przekaźnika komunikacji laserowej NASA (LCRD) był przełomową inicjatywą, która z powodzeniem transmitowała wideo w ultrawysokiej rozdzielczości między przestrzenią kosmiczną a Ziemią.

Oczekuje się, że technologia ta odegra kluczową rolę w nadchodzących misjach NASA Artemis i Mars, zapewniając wymianę danych w czasie rzeczywistym o dużej przepustowości.

W międzyczasie Airbus poczynił znaczne postępy w realizacji projektu TELEO, demonstrując połączenie optyczne o przepustowości 10 Gb/s między satelitą geostacjonarnym, a stacjami naziemnymi. Ponadto terminal komunikacyjny Ultra Air Laser ma na celu ustanowienie szybkich połączeń laserowych między samolotami, a satelitami, co może zmienić łączność lotniczą.

Innowacje przemysłowe: Marvell i Mitsubishi Electric

Branża elektroniczna jest również świadkiem znaczącego wkładu ze strony dużych firm technologicznych. W 2024 roku firma Marvell Technology wprowadziła na rynek Nova 2, pierwszy na świecie koherentny optyczny procesor DSP o rozdzielczości 1,6 terabita, który obsługuje 200G na linię elektrycznych i optycznych wejść/wyjść. Oczekuje się, że ta innowacja zwiększy wydajność transmisji danych satelitarnych, co ma kluczowe znaczenie dla zastosowań opartych na sztucznej inteligencji i przetwarzania w chmurze w kosmosie.

Z kolei Mitsubishi Electric z powodzeniem wprowadziło na orbitę niedrogi moduł źródła laserowego, działający niezawodnie przez pół roku. Rozwiązanie toruje drogę dla bardziej przystępnych cenowo kosmicznych sieci optycznych o dużej przepustowości, dzięki czemu komunikacja laserowa będzie bardziej dostępna.

Trendy w sieciach optycznych i ich rola w ewolucji rynku

Europejski wyścig kosmiczny: Airbus, Thales i Leonardo

Dostrzegając potencjał sieci satelitarnych opartych na laserach, europejscy giganci lotniczy Airbus, Thales i Leonardo zaangażowali się w rozmowy w celu utworzenia strategicznego sojuszu. Ich współpraca ma na celu wzmocnienie konkurencyjności Europy w branży satelitarnej, szczególnie w odpowiedzi na dominację inicjatyw prowadzonych przez USA i sektor prywatny, jak Starlink. Sojusz ten może znacznie przyspieszyć przyjęcie optycznego procesora DSP w europejskiej infrastrukturze kosmicznej.

Przyszłość komunikacji laserowej

Pomimo swoich zalet, laserowa komunikacja satelitarna nadal stoi przed wyzwaniami. Zakłócenia atmosferyczne, wymogi na precyzyjne wyrównanie oraz oszczędności energii pozostają krytycznymi przeszkodami. Jednak ciągłe badania i postęp technologiczny nadal udoskonalają i optymalizują te systemy, dzięki czemu stają się one coraz łatwiejsze do powszechnego wdrażania.

Wraz z postępem technologii transceiverów DSP z koherentnym procesorem optycznym, sieci naziemne będą w przeważającej mierze oparte na jeszcze lepszych technikach laserowych (lub mieszance technologii wykorzystujących fotonikę krzemową albo fosforek indu jako dominujące źródła w celu zmniejszenia śladu węglowego i zużycia energii wymaganej dla sieci transportowych), wychodząc naprzeciwko potrzebom na wzajemne połączenia GPU w centrach danych lub poza nimi, od bezproblemowej komunikacji w głębokim kosmosie do obsługi sieci sztucznej inteligencji nowej generacji.



Do klubu dołącza telekomunikacyjny DSP

W styczniu 2024 roku Nokia Bell Labs została wybrana przez amerykańską Agencję Zaawansowanych Projektów Badawczych w Obszarze Obronności (DARPA) do udziału w programie 10-letniej architektury księżycowej (LunA-10). Inicjatywa ta ma na celu zaprojektowanie zintegrowanej infrastruktury wielousługowej, która będzie wspierać zrównoważoną gospodarkę księżycową do 2035 roku. Rola Nokii polega na opracowaniu niezawodnej i wydajnej infrastruktury komunikacyjnej, niezbędnej do prowadzenia działalności przemysłowej na Księżycu i eksploracji naukowej.

Z kolei we wrześniu Nokia, we współpracy z Grupą OTE, osiągnęła podwójny rekord świata w szybkości transmisji optycznej na bardzo duże odległości.

Wykorzystując technologię PSE-6s (Super-Coherent Photonic Service Engine) szóstej generacji, sieć z powodzeniem transmitowała 800 Gb/s na odległość 2580 km i 900 Gb/s na odległość 1290 km.

W grudniu Nokia i Aramco przeprowadziły próbę terenową, uzyskując transmisję optyczną z prędkością 2,4 Tb/s przy użyciu technologii PSE-6s. Zademonstrowano wdrożenie z pełną pojemnością kart liniowych Nokii pokazując ogromny potencjał w zakresie zwiększenia wydajności i pojemności istniejącej infrastruktury sieci światłowodowej Aramco.

Inicjatywy te podkreślają aktywne zaangażowanie firmy Nokia w rozwój technologii optycznego koherentnego procesora DSP i podsystemów optycznych (z zintegrowaną fotoniką), wymaganych zarówno do komunikacji naziemnej, jak i pozaziemskiej.

Podsumowanie

Na podstawie naszych doświadczeń możemy wyciągnąć kilka wniosków. Chociaż sieci Quantum-Safe dopiero za jakiś czas zabezpieczą sieci podatne na ataki deszyfrowania kwantowego, to transformacja musi rozpocząć się już teraz, aby uniknąć zagrożeń w przyszłości. Z kolei szybki postęp w koherentnym optycznym cyfrowym przetwarzaniu sygnału (DSP) w komunikacji satelitarnej i optycznych podsystemach, sygnalizuje wyznaczanie nowej ery w telekomunikacji. Ponieważ sieci naziemne i pozaziemskie uwspólniają zastosowanie koherentnych łączy optycznych o dużej przepustowości i dalekim zasięgu, dostawcy usług telekomunikacyjnych mogą współpracować nad nowymi modelami konkurencyjnych usług.



Co to oznacza dla operatorów?

1. Rozpocznij automatyzację sieci i wykorzystaj jej możliwości w każdym aspekcie operacyjnym cyfrowej transformacji węzłów i sieci

Wykorzystanie najnowszych optycznych koherentnych trancceiverów DSP i automatyzacji sieci, pozwoli na efektywne kosztowo większe przepustowości i elastyczne wdrożenia o bardzo niskich opóźnieniach. Dostawcy usług telekomunikacyjnych mogą integrować szybkie technologie fotoniczne ze swoimi sieciami światłowodowymi, aby sprostać rosnącemu zapotrzebowaniu na ultraszybkie usługi transmisji danych o niskich opóźnieniach.

2. Przygotuj się do hybrydowych sieci satelitarnych i naziemnych

Przyszłość komunikacji leży w modelach hybrydowych, w których naziemne łączy światłowodowe i satelitarne płynnie ze sobą współpracują. Dostawcy telekomunikacyjni powinni inwestować w integrację laserowej łączności satelitarnej ze swoją infrastrukturą, aby zapewnić stabilny, globalny zasięg, szczególnie na obszarach o niedostatecznym zasięgu lub bardzo odległych.

3. Wykorzystaj sztuczną inteligencję i automatyzację do optymalizacji sieci

Koherentna optyczna technologia DSP stanowiąca podstawowy wspólny element i mogąca współpracować z sieciami autonomicznymi (w dużym lub pełnym stopniu) i wykorzystująca sztuczną inteligencję zwiększa wydajność oraz zmniejsza koszty operacyjne. Analizując ogromne ilości danych w czasie rzeczywistym, sztuczna inteligencja może optymalizować ścieżki transmisji optycznej, przewidywać awarie i zapewniać maksymalny czas pracy.

4. Skoncentruj się na bezpieczeństwie komunikacji wolnej od zakłóceń

Komunikacja oparta na laserze zapewnia wyższy poziom bezpieczeństwa w porównaniu z tradycyjnymi metodami opartymi na częstotliwości radiowej, dzięki czemu idealnie nadaje się do zastosowań rządowych, obronnych i korporacyjnych. Sieci tego typu mogą z łatwością dostosować plany z domeny Quantum Safe do dowolnych klasycznych topologii i segmentów. Dostawcy usług telekomunikacyjnych powinni zacząć stosować rozwiązania w zakresie bezpiecznej transmisji optycznej, aby sprostać rosnącemu zagrożeniom kwantowym, dzięki szyfrowanym, szybkim transferom danych.

Wniosek: Przyszłość należy do sieci optycznych

Dostawcy usług telekomunikacyjnych, którzy zastosują technologię Quantum Safe oraz najnowsze koherentne optyczne procesory DSP, staną na czele kolejnej fali bezpiecznych sieci o wysokiej wydajności. Niezależnie od tego, czy chodzi o komunikację laserową w przestrzeni kosmicznej, czy o szybką naziemną transmisję optyczną, przyszłość należy do tych, którzy integrują najnowocześniejsze rozwiązania fotoniczne ze swoją infrastrukturą. Czas wykorzystać te innowacje w codziennych wdrożeniach.

Trendy w sieciach optycznych i ich rola w ewolucji rynku



Źródła i inspiracje

- <https://omdia.tech.informa.com/om122772/telco-network-and-service-automation-market-tracker-report--2024>
- <https://www.lightreading.com/network-automation/open-automated-and-programmable-transport-networks-2024-heavy-reading-survey>
- <https://telecom.economictimes.indiatimes.com/news/telecom-equipment/optical-network-automation-save-telcos-up-to-81-in-network-service-management-costs-analysis-mason-nokia-study/107320849>
- <https://www.globenewswire.com/en/news-release/2024/03/21/2849925/0/en/Nokia-enhances-optical-network-automation-capabilities-to-help-network-operators-reduce-CAPEX-and-OPEX-increase-revenues>
- <https://www.nokia.com/about-us/news/releases/2024/12/20/nokia-and-turkcell-demonstrate-industry-leading-quantum-safe-protection-for-mobile-subscribers/>
- <https://www.nokia.com/about-us/news/releases/2024/12/11/nokia-and-sk-broadband-deploy-quantum-secure-network-to-protect-korea-hydro-and-nuclear-powers-it-infrastructure/>
- <https://www.nokia.com/industries/quantum-safe-networks/>
- <https://www.forbes.com/sites/nokia-industry-40/2024/08/12/quantum-computing-is-coming-heres-what-needs-to-happen-first/>
- <https://www.youtube.com/watch?v=QIDOt4lp4xl&t=1s>
- <https://www.wsj.com/articles/q-day-is-coming-its-time-to-worry-about-quantum-security-ca88c576>
- <https://www.thetimes.co.uk/article/battle-begins-to-stop-quantum-computers-smashing-cyber-defences-rzmlwqw7f>
- <https://www.reuters.com/technology/cybersecurity/europol-body-banks-should-prepare-quantum-computer-risk-now-2025-02-07/>
- <https://www.theverge.com/2024/7/24/24205469/nasa-lasers-lcrd-optical-communication-international-space-station>
- <https://emea.mitsubishielectric.com/en/news/releases/global/2024/0919-a/index.html>
- <https://www.prnewswire.com/news-releases/marvell-launches-products-technology-and-partnerships-at-ofc-2024-to-scale-optical-technology-for-accelerated-infrastructure-302099781>
- <https://www.airbus.com/en/newsroom/news/2024-12-airbus-and-partners-demonstrate-very-high-speed-optical-link-between-earth>
- <https://www.aerospacetestinginternational.com/news/space/airbus-moves-ultraair-laser-based-satellite-communications-program-to-flight-testing-phase.html>
- <https://www.ft.com/content/650d5e2a-65c4-4c72-bf66-92ccdf25f5f7>
- <https://www.nokia.com/about-us/news/releases/2024/01/23/nokia-selected-by-darpa-to-design-communications-services-infrastructure-framework-for-future-lunar-economy/>
- <https://www.nokia.com/about-us/news/releases/2024/09/12/nokia-and-ote-group-set-dual-world-record-optical-transmission-rates-over-ultra-long-distances/>
- <https://www.nokia.com/about-us/news/releases/2024/12/05/nokia-and-aramco-successfully-achieve-first-24tbs-optical-transmission/>

Światłowodowe systemy czujnikowe – nowe możliwości i szanse dla operatorów sieci



Sylwia Choma
Starszy Specjalista
Rozwoju Sieci i Usług
Orange



Andrzej Cąkała
Główny Architekt
Sieci i Usług
Orange

Od kilkunastu lat jesteśmy w Polsce świadkami intensywnej rozbudowy sieci światłowodowej, która dokonuje się głównie za sprawą operatorów telekomunikacyjnych inwestujących w sieci FTTx, ale nie tylko. Swoją infrastrukturę światłowodową, głównie do celów monitoringu wizyjnego, automatyki i sterowania urządzeniami infrastruktury teletechnicznej, budują również jednostki samorządu terytorialnego, dostawcy energii elektrycznej, gazu itp. To wszystko powoduje, że światłowód stał się wszechobecny w otaczającej nas przestrzeni i jest go wystarczająco dużo, by mógł być wykorzystany do innych celów niż dostarczanie usług telekomunikacyjnych czy sterowanie automatyką przemysłową. Szczególnie, gdy obecna sytuacja geopolityczna jest zmienna i powoduje, że kwestie ochrony kluczowych dla każdego państwa obiektów i instalacji stają się coraz bardziej istotne. Jest to więc potencjalna szansa na wykorzystanie wolnych zasobów sieci światłowodowej w zupełnie nowej roli, co może stać się też dodatkowym źródłem przychodu dla właścicieli



takiej infrastruktury, w szczególności gdy przebiega ona w pobliżu lub wręcz bezpośrednio przez strefy czy budynki wymagające specjalnej ochrony.

Czujnikowe zastosowania światłowodów znane są równie długo, jak same światłowody. Mnogość dostępnych rozwiązań technicznych wynika z różnorodności mierzonych wielkości fizycznych, typu światłowodu, miejsca pomiaru, tego czy pomiar jest punktowy czy rozproszony na większym dystansie itp.

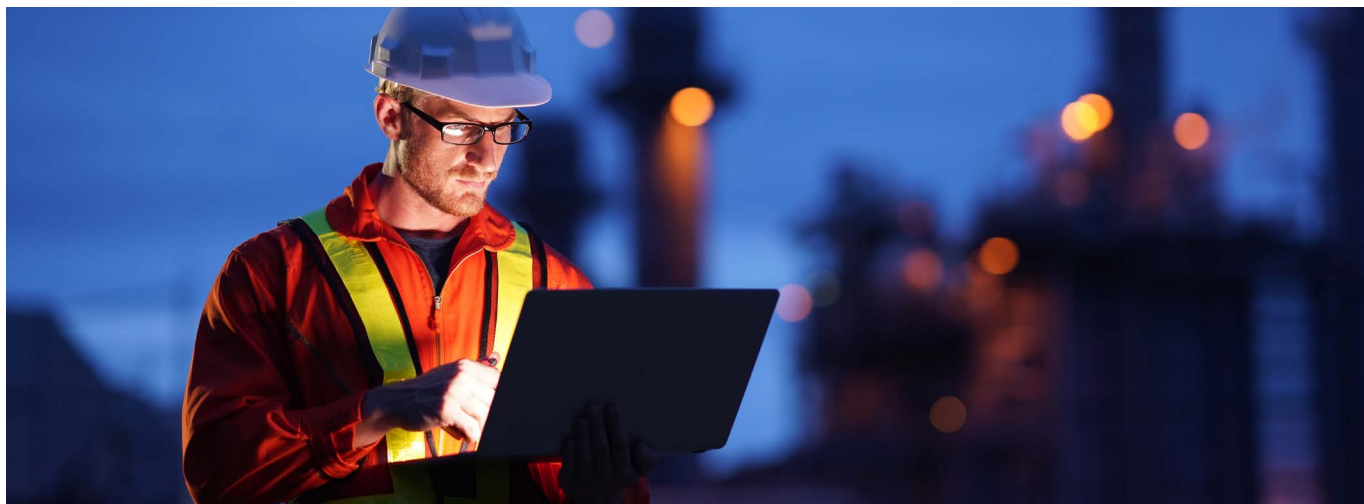
Przykładem prostego systemu pracującego w ten sposób może być tor światłowodowy podłączony do reflektometru OTDR (ang. Optical Time Domain Reflectometry). OTDR jest powszechnie stosowanym przyrządem do charakteryzowania parametrów toru światłowodowego (długość, tłumienie, lokalizacja i tłumienie zdarzeń itp.), ale łatwo można wyobrazić sobie nieco inne jego zastosowanie, gdzie światłowód jest świadomie wystawiony na bezpośrednie oddziaływanie mechaniczne otaczającego środowiska, a te generują w nim efekty makrozgięciowe, które ujawniają się w postaci punktowych lub rozproszonych zmian tłumienia w torze. OTDR pracujący w trybie ciągłym lub wykonując pomiary w krótkich odstępach czasowych jest w stanie zlokalizować te zmiany, podać ich dokładne położenie, a w korelacji z danymi map cyfrowych, ustalić dokładną lokalizację na monitorowanym terenie.

W niektórych przypadkach wzrost tłumienia można powiązać z wielkością oddziaływania zewnętrznego i w ten sposób dokonywać kategoryzacji naruszeń obiektów je powodujących. Metoda, choć tania w implementacji, charakteryzuje się mocno ograniczoną przydatnością ze względu na niską czułość i przede wszystkim punktowe wykrywanie oddziaływań zewnętrznych na światłowód.

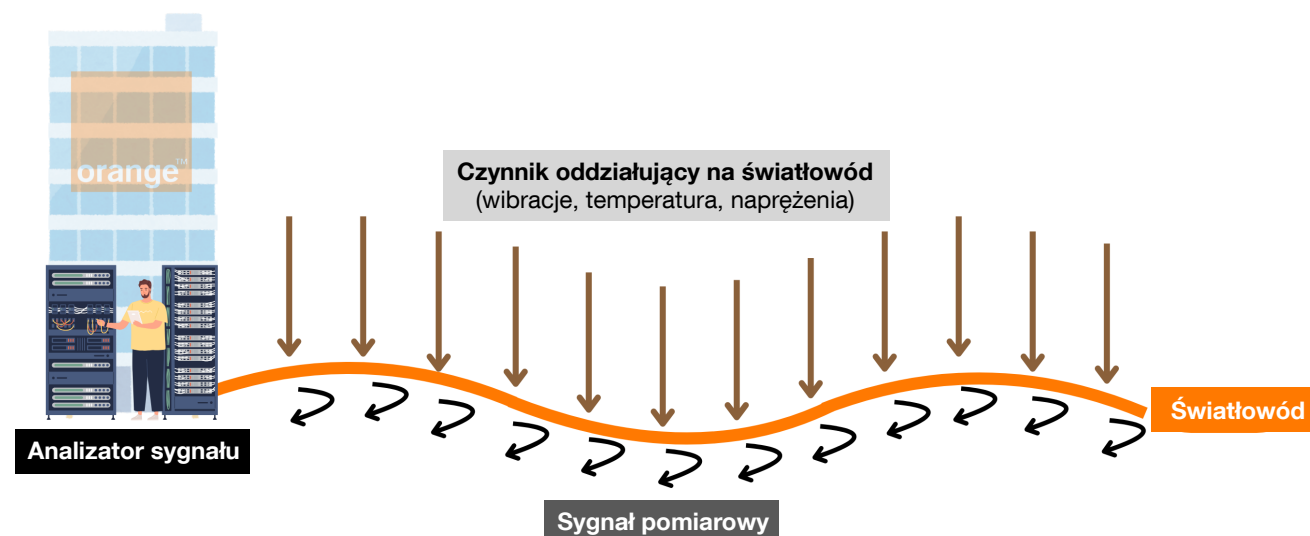
Światłowodowe systemy czujnikowe – nowe możliwości i szanse dla operatorów sieci

Z perspektywy właściciela/operatora sieci światłowodowej najciekawszą grupą możliwych do wykorzystania rozwiązań jest rodzina systemów czujnikowych DOFs (ang. Distributed Optical Fiber Sensors), której cechą charakterystyczną jest to, że światłowód jest jednocześnie czujnikiem i medium przenoszącym optyczny sygnał pomiarowy.

Drugą ważną cechą tej rodziny jest ciągłość przestrzenna pracy światłowodu jako czujnika, co oznacza, że każdy, nawet najmniejszy jego odcinek ma swój udział w modyfikowaniu parametrów przenoszonego sygnału optycznego. Wielkość tych zmian jest ściśle skorelowana z charakterem oddziaływania zewnętrznego na włókno (Rysunek poniżej).



System czujnikowy DOFs



W komercyjnie dostępnych na rynku rozwiązaniach dominują systemy czujnikowe DAS (ang. Distributed Acoustic Sensing), w których wybrane cechy sygnału pomiarowego powracającego ze światłowodu do układu nadawczo-odbiorczego zmieniają się pod wpływem zjawisk występujących we włóknach światłowodowych, np.: rozpraszania Ramana, rozpraszania Brillouina, rozpraszania Rayleigh'a itp. Zjawiska te, mniej lub bardziej, wpływają na transmitowany sygnał pomiarowy i wykazują silną korelację z rodzajem oddziaływania zewnętrznego: temperaturą, wibracjami, falą dźwiękową.

Sygnał, powracający ze światłowodu do urządzenia nadawczo-odbiorczego, jest poddawany analizie, której wynikiem jest użyteczna informacja na temat wystąpienia zdarzenia, jego siły i zmiany w czasie.

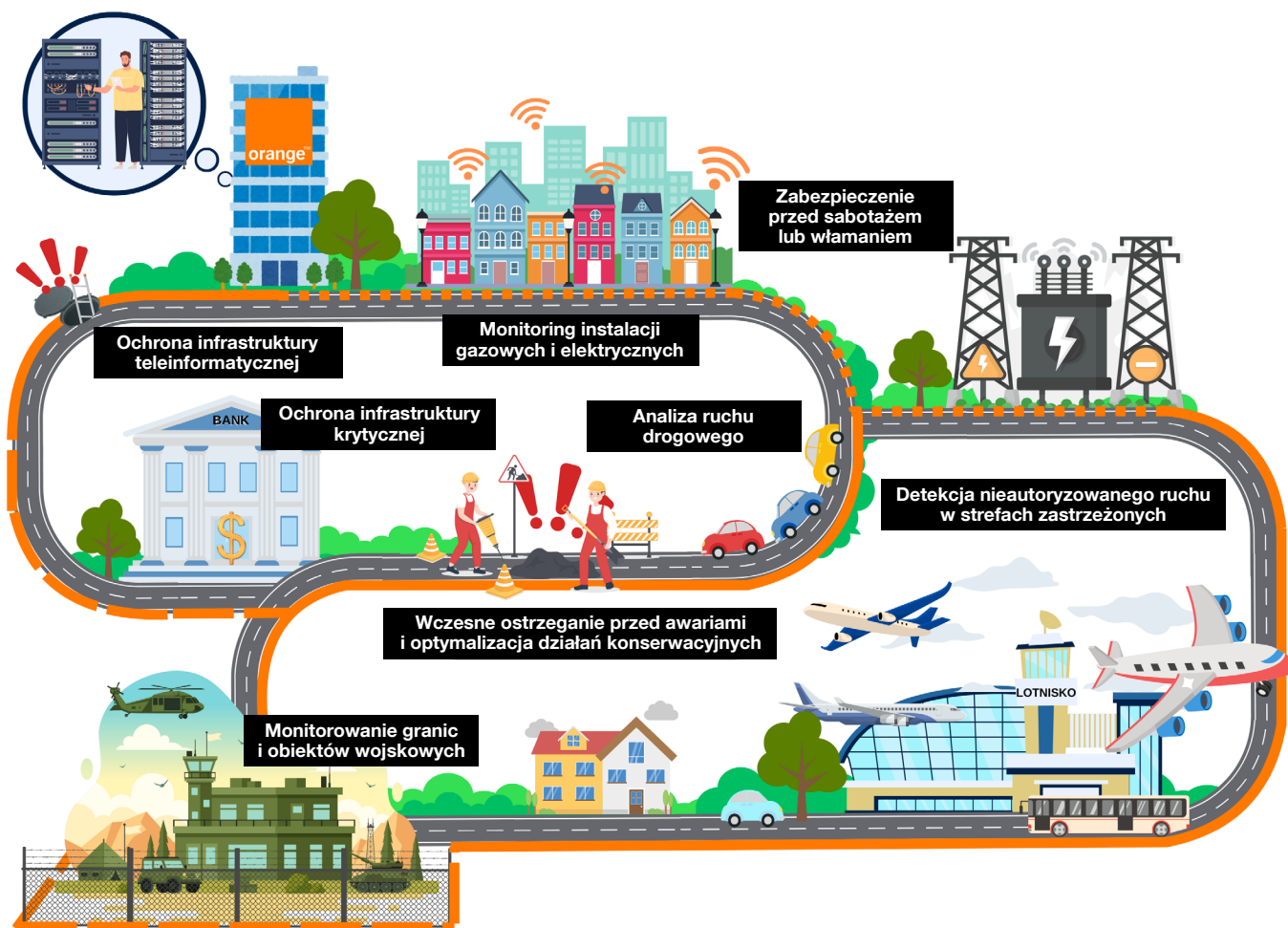
Światłowodowe systemy czujnikowe – nowe możliwości i szanse dla operatorów sieci

Dzięki odpowiednim algorytmom i konfiguracji systemu czujnikowego możliwa jest identyfikacja typu obiektu (np.: człowiek, samochód, pociąg, dron) i charakteru powodowanego naruszenia w monitorowanym obszarze (np. przejazd auta, kopanie w gruncie). Różne scenariusze wykorzystania systemów czujnikowych przedstawiono na rysunku obok.

Od zabezpieczania elementów infrastruktury telekomunikacyjnej w celu wykrywania nieautoryzowanego dostępu poprzez ochronę obiektów lub stref o szczególnym znaczeniu: lotnisk, urządzeń energetycznych, granic państwowych. Systemy czujnikowe DAS mogą nie tylko informować w czasie rzeczywistym o zbliżaniu się obiektu do chronionej strefy zanim jeszcze dojdzie do jej naruszenia, ale również identyfikować klasę obiektu, wielkość, śledzić tor jego przemieszczania.

Jak każdy system pomiarowy, a DAS takim jest, ma również swoje ograniczenia, a różnorodność scenariuszy wykorzystania tych systemów jest w zasadzie ograniczona dwoma głównymi czynnikami: możliwością wykorzystania zainstalowanych światłowodów jako czujników lub koniecznością wybudowania nowych oraz kosztami zakupu, instalacji i utrzymania systemu. Pierwsze ograniczenie można prosto pokonać korzystając z istniejących zasobów sieci światłowodowej lub angażując operatorów do budowy dedykowanej infrastruktury. A finanse? No cóż... w przypadku konieczności ochrony infrastruktury krytycznej też nie są barierą nie do pokonania.

Przykłady możliwości wykorzystania systemów DAS



„Copper Switch Off” czyli wycofywanie z eksploatacji sieci miedzianych



Grzegorz Kuźmicz
Ekspert ds. Analiz
Rynków Europejskich
Orange

W ostatnich latach „Copper Switch Off” stał się ważnym tematem wielu konferencji branżowych nie tylko w Europie, ale i na świecie. Często wspomina się o nim w kontekście cyfrowej transformacji Europy. Samo pojęcie oznacza wycofywanie z eksploatacji sieci miedzianych, które z biegiem czasu zostały zastąpione nie tylko przez sieci stacjonarne nowszych generacji, ale również sieci bezprzewodowe umożliwiające uzyskanie wyższych parametrów usług niż te dostępne na parach miedzianych. Rozwój nowych technologii telekomunikacyjnych na przestrzeni ostatnich lat oraz inwestycje w bardziej nowoczesne sieci powoduje, że użytkownicy końcowi mają obecnie dostępne alternatywy, co wiąże się ze stopniowym ich odpływem z sieci miedzianych do sieci stacjonarnych o bardzo dużej przepustowości oraz do sieci mobilnych. Z powodu malejącego popytu na usługi świadczone na parach miedzianych nawet dostawcy urządzeń telekomunikacyjnych stopniowo wycofują się ze wspierania starych technologii opartych o miedziane medium fizyczne na rzecz nowszych rozwiązań telekomunikacyjnych.

Na świecie możemy zaobserwować już wiele przykładów wycofywania starych sieci miedzianych z eksploatacji. Praktycznie nie sposób znaleźć operatora, który posiada sieć dostępową opartą o pary miedziane i nie zastanawia się nad wycofaniem ich z eksploatacji. Już wielu z tych operatorów jest bardzo zaawansowanych w działaniach likwidacyjnych. Jeżeli przyjrzymy się wyłącznie krajom Unii Europejskiej oraz Wielkiej Brytanii to pojawia się bardzo zróżnicowany obraz.

Jak podaje raport opublikowany przez FTTH Council Europe z grudnia 2024 r.¹, w niektórych państwach członkowskich zaczęto już wyłączać swoją sieć miedzianą, podczas gdy w innych krajach jeszcze nie ogłoszono publicznie planu wycofania tej sieci z eksploatacji. W 12 krajach operatorzy mają plan całkowitego wyjścia z sieci miedzianej, natomiast jedynie w 5 krajach określono datę wycofania z eksploatacji całej infrastruktury miedzianej.



1) Copper Switch-Off Tracker, December 2024
<https://www.ftthcouncil.eu/resources/all-publications-and-assets/2317/copper-switch-off-tracker-decommissioning-copper-in-the-european-union-and-the-united-kingdom>

„Copper Switch Off” czyli wycofywanie z eksploatacji sieci miedzianych

Kraje, w których ogłoszono plany wycofania z eksploatacji sieci miedzianych (Unia Europejska z Wielką Brytanią)².

Kraj	Data wyłączenia całej sieci miedzianej
Belgia	Nie określono
Cypr	Nie określono
Dania	2030
Finlandia	2025 (operator DNA)
Francja	2030
Węgry	Nie określono
Luksemburg	2030
Holandia	Nie określono
Portugalia	Nie określono
Hiszpania	2025
Szwecja	2026
Wielka Brytania	2027 – określono tylko dla usług głosowych PSTN

2) Copper Switch-Off Tracker, December 2024
<https://www.ftthcouncil.eu/resources/all-publications-and-assets/2317/copper-switch-off-tracker-decommissioning-copper-in-the-european-union-and-the-united-kingdom>

Orange Polska prowadzi działania zmierzające do wycofania z eksploatacji sieci miedzianej, ale na bardzo ograniczonych obszarach kraju. Praktyka europejska pokazuje, że nie ma możliwości wycofania zasięgu całej sieci miedzianej z dnia na dzień. Proces likwidacji sieci miedzianej jest bardzo skomplikowany i angażujący duże zasoby przedsiębiorstwa, zatem należy zakładać, iż jest to proces wieloletni. Doświadczenia europejskie w zakresie wycofywania infrastruktury miedzianej z eksploatacji potwierdzają ten fakt. Np. hiszpańska Telefonica rozpoczęła proces w 2014 i dopiero w bieżącym roku spodziewane jest wycofanie z eksploatacji ostatnich przełącznic głównych. W związku z tym, w Hiszpanii cały proces trwa już 10 lat i termin pełnego wyjścia z eksploatacji sieci miedzianych był w przeszłości odraczany. Innym ciekawym przypadkiem jest Szwecja, która rozpoczęła swój proces w 2015 roku. Pełne wyłączenie sieci miedzianej w tym kraju spodziewane jest w roku 2026, zatem ten kraj również jest liderem i dołącza do grupy krajów najbardziej zaawansowanych w wyłączaniu sieci miedzianej w Europie. Zakładając, że termin pełnego wyłączenia sieci miedzianej zostanie dotrzymany to cały proces w Szwecji będzie trwał aż 11 lat.

Niezależnie od powyższych przykładów są też kraje w Europie, które nie mają jeszcze skonkretyzowanych planów jak np. Wielka Brytania. W tym kraju określono jedynie termin pełnego wyłączenia usług PSTN w 2027 roku, które w pełni zastąpiły rozwiązania oparte na VoIP lub sieci mobilnej. Jest to swoistego rodzaju przykład pełnego wycofania z eksploatacji jedynie przestarzałej technologii na potrzeby świadczenia usług głosowych, co raczej należy postrzegać jako wstęp do wyłączenia całej sieci miedzianej. Jednym z najmniej zaawansowanych krajów w Europie są Niemcy, które w związku



z wdrożeniem technologii VDSL Vectoring wykonały pewne działania optymalizacyjne na sieci miedzianej, niemniej jednak moim zdaniem nie powinno się tego kwalifikować jako rozpoczęcie procesu wyłączania sieci miedzianej.

Orange inwestuje w nowoczesne technologie – 5G, światłowody oraz korzysta z usług hurtowych innych operatorów infrastruktury na rynku, co pozwala wyłączać nieaktywne obiekty, infrastrukturę, na której świadczymy usługi w starszych technologiach. Niezależnie od powyższego, już teraz zachęcamy naszych klientów Operatorów do skorzystania z dostępnych ofert hurtowych Orange w celu migracji usług świadczonych na parach miedzianych do bardziej nowoczesnych i wypróbowanych przez rynek usług opartych na światłowodzie lub technologii mobilnej, w tym 5G:

- **BSA** – <https://hurt-orange.pl/operatorzy-krajowi/uslugi/hurtowe-uslugi-abonenckie/bsa/>
- **LLU** – <https://hurt-orange.pl/operatorzy-krajowi/uslugi/hurtowe-uslugi-abonenckie/local-loop-unbundling-llu/>
- **MVNO** – <https://hurt-orange.pl/operatorzy-krajowi/uslugi/mvno/>

RCS-ie, czy „jesteś lekiem na całe zło”?



Radosław Turek
Kierownik
Produktów
Hurtowych
Orange



Jerzy Klimaszewski
Prezes Zarządu
Tide Software

Komu po przeczytaniu tytułu, od razu przypomniał się refren jednego z najpiękniejszych szlagierów Krystyny Prońko? Utwór powstał zimą 1982 roku, a słowa piosenki napisał Bogdan Olewicz, który w zakamuflowanej formie – z uwagi na powszechną w tym czasie cenzurę – nawiązał do tego trudnego okresu w historii naszego kraju. Co jednak wspólnego ma ten przebój, który zapisał się złotymi nutami w dorobku polskiej muzyki ze światem telekomunikacji?

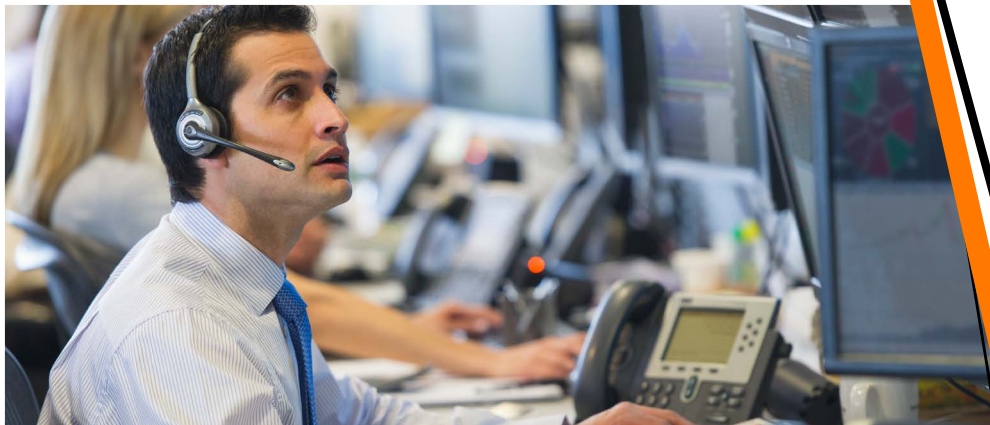
Po ponad 40 latach chyba nic nie stracił na swojej aktualności. Zmieniło się otoczenie i technologia, ale jego refren pozostaje wciąż aktualny. Skuteczne dotarcie do odbiorców w obecnych czasach, choć możliwości i narzędzi mamy więcej, paradoksalnie jest coraz trudniejsze. Stawiając tezę, podzielimy się infografiką z danymi znalezionymi w serwisie Spider's Web, która pokazuje jaka ilość informacji atakuje nas każdego dnia.



W tym miejscu należy odpowiedzieć sobie na kilka istotnych pytań:

- Czy jesteśmy w stanie przy takim natłoku informacji przebić się ze swoimi komunikatami?
- Czy nasi klienci mający darmowe konta e-mail w największych, komercyjnych serwisach są w stanie wyłowić nasz mail w dziesiątkach wiadomości reklamowych, które są wysyłane przez partnerów tych serwisów?
- Czy nasi klienci wciąż chętnie czytają wiadomości reklamowe wysyłane SMS-ami?

„Zróbmy więc kolejną obdzwonkę klientów!” – to najprostsze rozwiązanie. Tyle tylko, że po kilku połączeniach, nawet nowe numery kupione od operatora, błyskawicznie zostają oznaczone przez odbiorców jako spam. Kolejny klient, do którego zadzwonimy będzie miał już ostrzeżenie na swoim telefonie o potencjalnym spamie.



RCS-ie, czy „jesteś lekiem na całe zło”?

„Ty w tej samej kurtce szósty rok...”

Czy w dalszym ciągu, jak w słowach wspomnianego przeboju, korzystamy ze znanych, wyeksploatowanych i coraz mniej skutecznych kanałów „legacy” w kontakcie z naszymi klientami? Odpowiedź na to pytanie brzmi: niestety tak.

W firmach wciąż obecne są gotowe, dawno temu zaimplementowane i ciągle te same procesy oraz kanały kontaktu z klientami. Często bez względu na to, jak skutecznie docierają z komunikatami do odbiorców. Duża część firm nie mierzy skuteczności, ponieważ najpowszechniej wykorzystywane dotąd kanały komunikacji mobilnej nie oferują możliwości sprawdzenia, czy wiadomość została wyświetlona na urządzeniu odbiorcy.

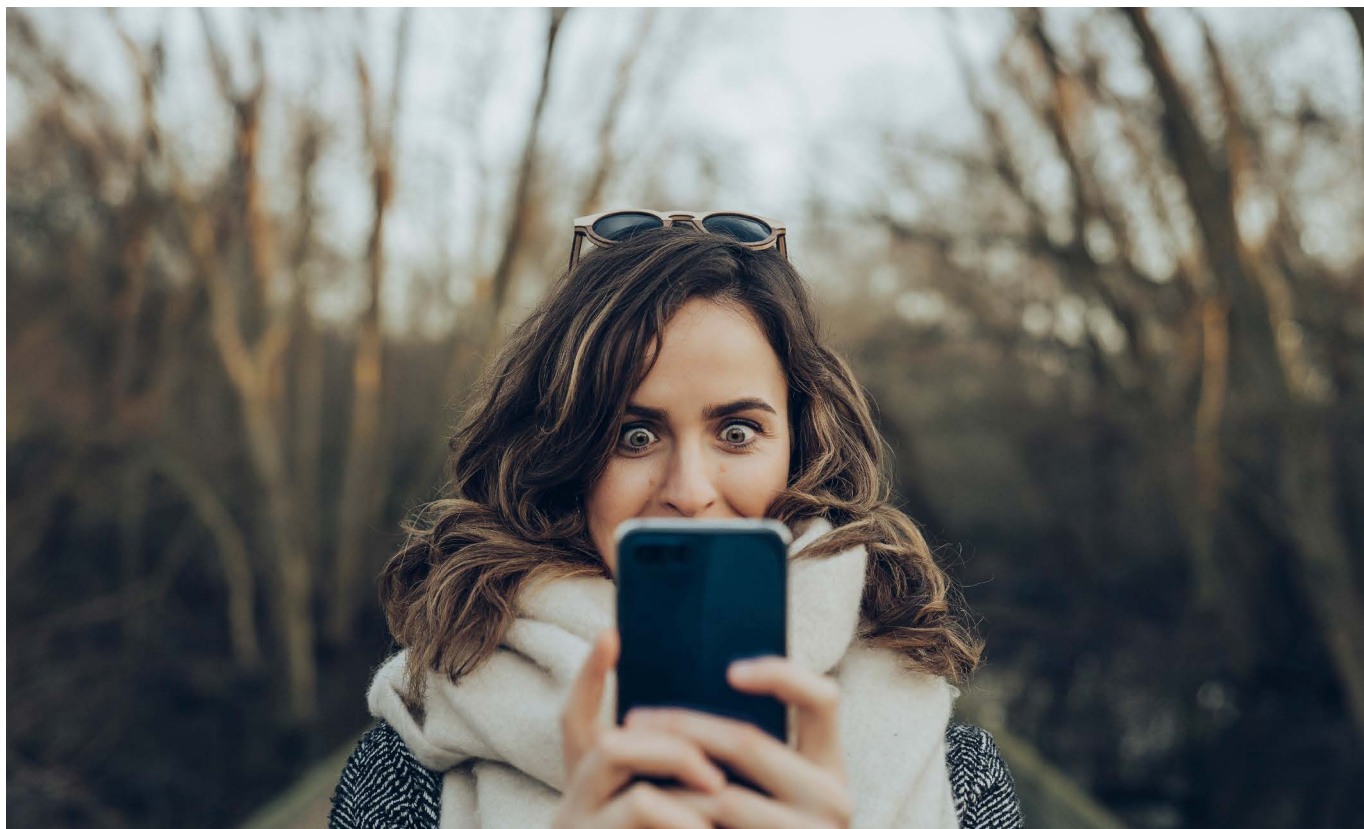
Można próbować e-mailem, ale również nie wszyscy potwierdzają odczytanie wiadomości.

Czy jest na to jakiś sposób? Oczywiście, że tak! Postaramy się odpowiedzieć na to pytanie w dalszej części artykułu, ale na początku przyjrzyjmy się obecnej sytuacji na rynku komunikacji elektronicznej.

„Jesteś gwiazdą w ciemności...”

Czy biorąc pod uwagę fakt, że do użytkowników dociera coraz więcej komunikacji niebezpiecznej – m.in. częste są próby wyłudzeń danych osobowych lub pieniędzy – jesteśmy w stanie skutecznie i bezpiecznie dotrzeć do nich z naszą informacją?

25 września 2023 roku weszła w życie Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej,



której celem jest przeciwdziałanie próbom phishing’u, smishingu, spoofing e-mail i CLI spoofing’u. Obliguje ona operatorów do implementacji zabezpieczeń przeciwdziałającym nadużyciom. Działania zostały podjęte we współpracy międzyoperatorskiej i z udziałem CERT. Celem jest nie tylko wdrożenie rozwiązania technologicznego, ale również edukacja użytkowników. I to ona ma kluczowe znaczenie.

O ile bowiem skutki wykorzystania samej technologii i mechanizmów blokujących nadużycia są natychmiastowe, to sam proces budowania świadomości i edukacji użytkowników jest długofalowy.

Niestety, kreatywność przestępców nie zna granic i na każdą próbę technicznej eliminacji zagrożeń, znajdują nowe sposoby dotarcia do klienta.

RCS-ie, czy „jesteś lekiem na całe zło”?

„Mówisz, że nikogo się nie boisz...”

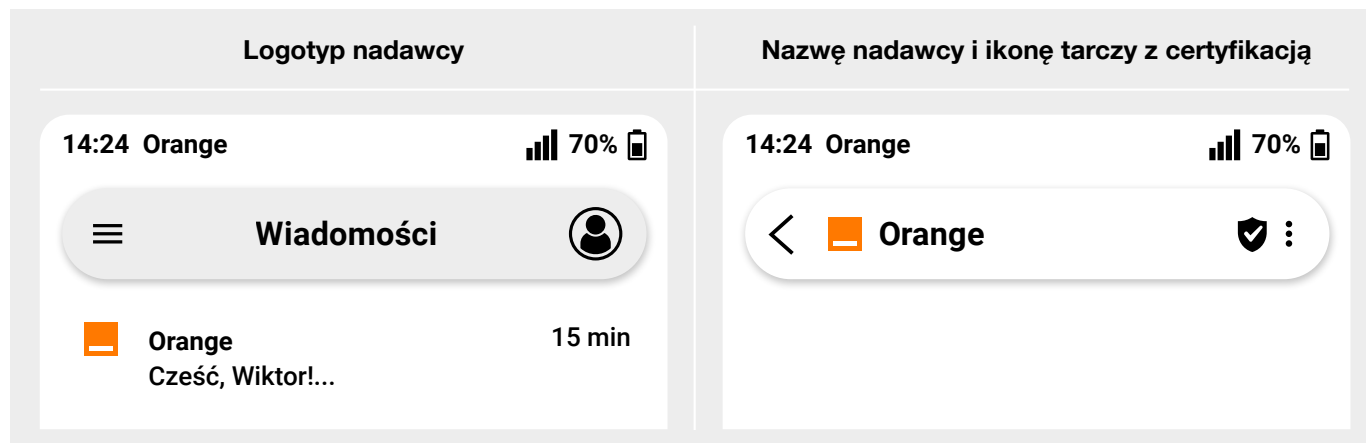
Poza działaniami prewencyjnymi, które zostały podjęte przez operatorów po uchwaleniu ustawy, bezpieczeństwu sprzyja również najnowsza technologia telekomunikacyjna udostępniona przez operatorów na rzecz rynku i podmiotów gospodarczych. Tradycyjne kanały komunikacji jak SMS czy MMS coraz częściej zastępowane są nowym, niewymagającym instalacji na telefonie dodatkowej aplikacji, kanałem RCS. Jest on w pełni kontrolowany przez operatora i pozwala na weryfikację nadawcy w komunikacji biznesowej (A2P) zanim dotrze ona do klienta. Czy w takim razie RCS stanie się narzędziem, którego zacząć obawiać się przestępcy? Czy ma potencjał, aby stanowić skuteczną odpowiedź na próby nadużyć z wykorzystaniem metod jak: phishing, smishing, spoofing e-mail i CLI spoofingu?

„Jesteś alfą, omegą, hymnem, kołędą...”

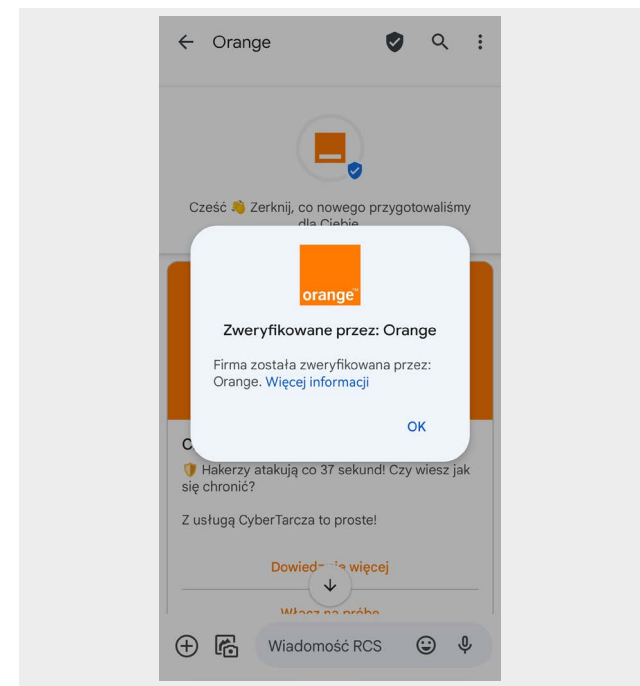
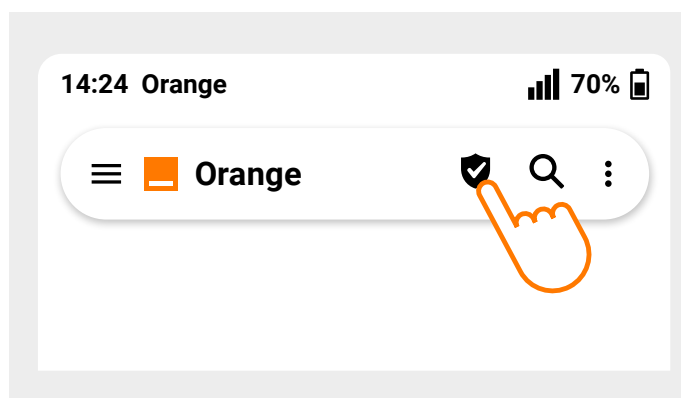
Smishing (także **SMS phishing** – definicja Wikipedii) to, wysłanie krótkiej wiadomości tekstowej (SMS), w której nadawca podszywa się pod inny podmiot, w celu nakłonienia odbiorcy tej wiadomości do określonego zachowania. W szczególności do przekazania danych osobowych, niekorzystnego rozporządzenia mieniem, otwarcia strony internetowej, inicjowania połączenia głosowego lub instalacji oprogramowania.

Przyjrzyjmy się w jaki sposób można wyeliminować problem smishingu za pomocą RCS Basic lub Single Message.

Każda wiadomość RCS A2P posiada następujące elementy:

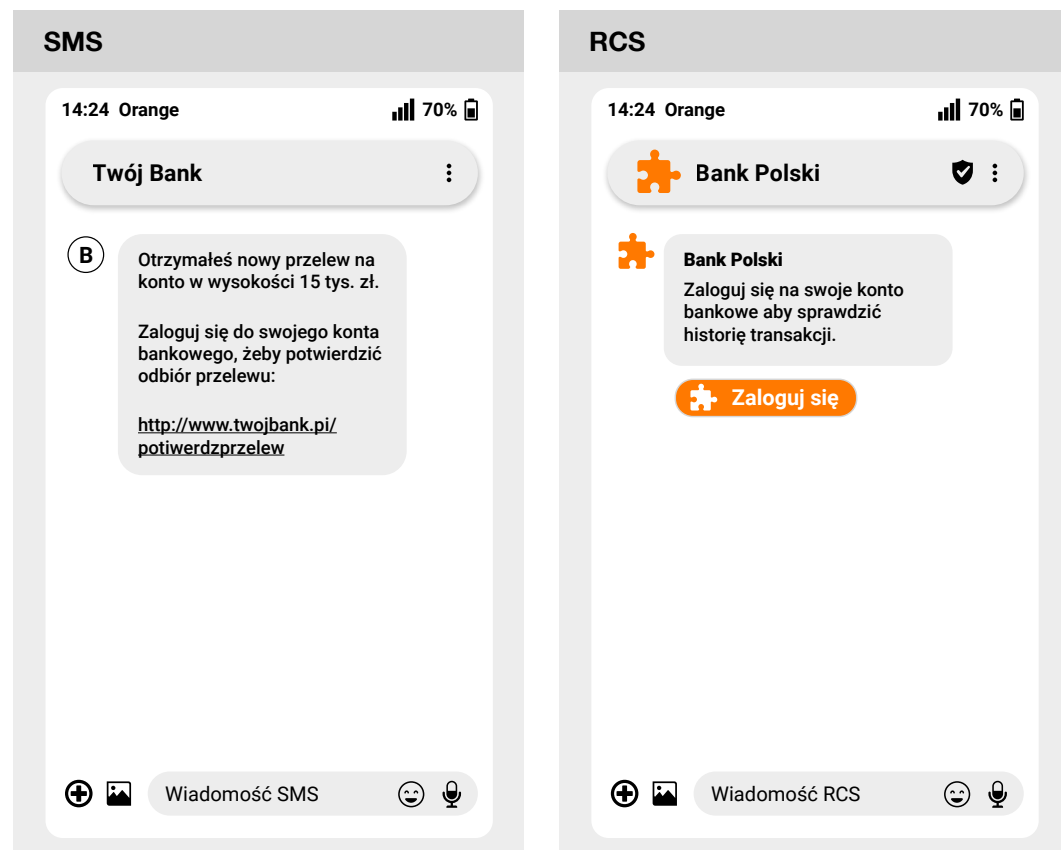


Każdy nadawca wysyłający RCS A2P jest weryfikowany przez Orange. Odbiorca może sprawdzić certyfikację w prosty sposób. Gdy kliknie na ikonkę tarczy na swoim telefonie, wyświetlona zostanie informacja o zweryfikowanym przez Orange nadawcy.



RCS-ie, czy „jesteś lekiem na całe zło”?

Jak może wyglądać przykładowa wiadomość RCS zawierająca bezpieczny link do naszej strony, który nie będzie wzbudzał niepokoju naszych odbiorców?



Bezpieczny link można przesłać:

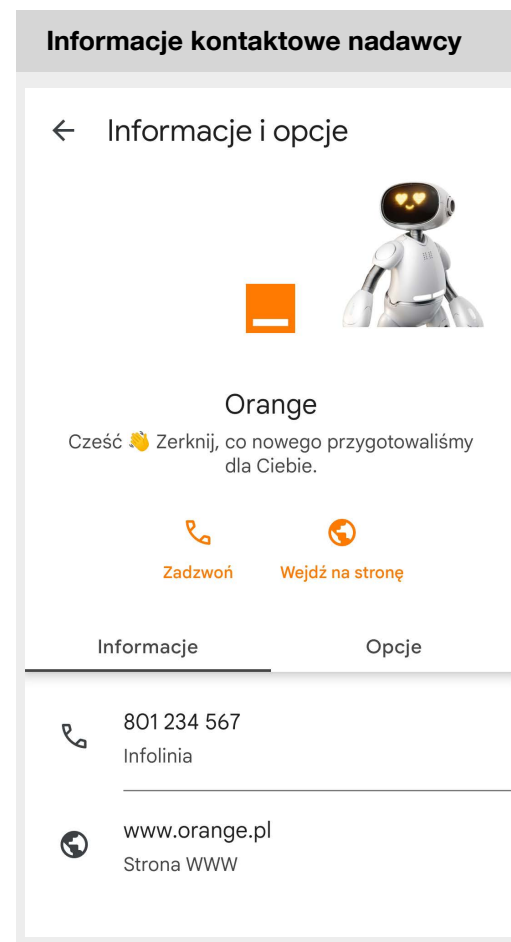
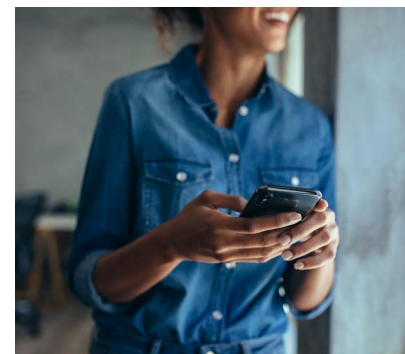
- w treści samej wiadomości,
- ale dzięki mechanizmom RCS również można umieścić na przycisku predefiniowanych odpowiedzi.

Za pomocą krótkiej wiadomości RCS (tzw. RCS Basic) możesz przesłać bezpiecznie nie tylko link do swojej strony, ale również kod autoryzacji np. w transakcji bankowej lub wykorzystywany w uwierzytelnianiu 2-składnikowym 2FA (two-factor authentication).

Phishing, tym razem skorzystajmy z definicji zamieszczonej w serwisie www.gov.pl, to jeden z najpopularniejszych typów ataków opartych o wiadomości e-mail lub SMS. Wykorzystuje inżynierię społeczną, czyli technikę polegającą na tym, że przestępcy internetowi próbują Cię oszukać i spowodować, abyś podjął działanie zgodnie z ich zamierzeniami. Cyberprzestępcy podszywając się m.in. pod firmy kurierskie, urzędy administracji, operatorów telekomunikacyjnych, czy nawet naszych znajomych, starają się wyłudzić nasze dane do logowania np. do kont bankowych lub używanych przez nas kont społecznościowych lub systemów biznesowych.

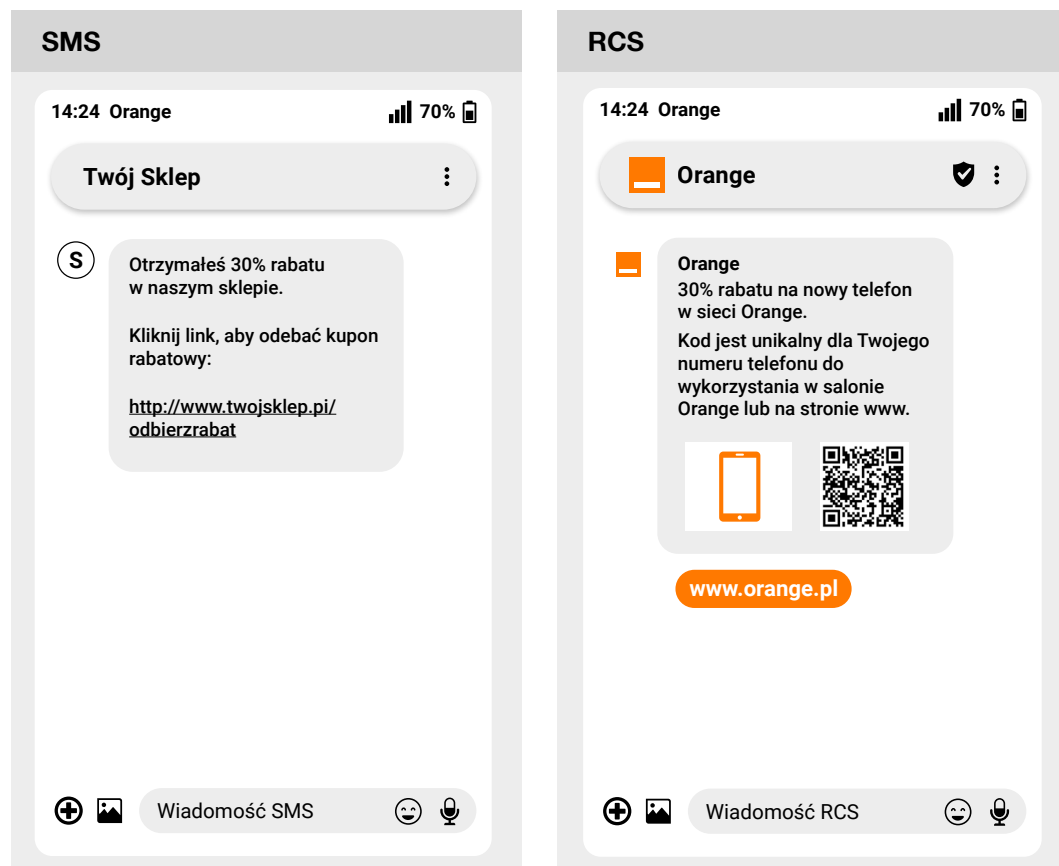
W jaki sposób wykorzystać RCS, aby nasz odbiorca miał pewność, że to my jesteśmy bezpiecznym nadawcą i nie jest to próba wyłudzenia danych?

Każdy typ wiadomości RCS (Basic, Single i Conversation) zawierają szczegółowe informacje kontaktowe do nadawcy (strona WWW, numer telefonu kontaktowego, adres e-mail czy linki do regulaminu i polityki prywatności wraz z logiem firmy), co daje pewność odbiorcy, że jest to zweryfikowany przez Orange i bezpieczny nadawca.

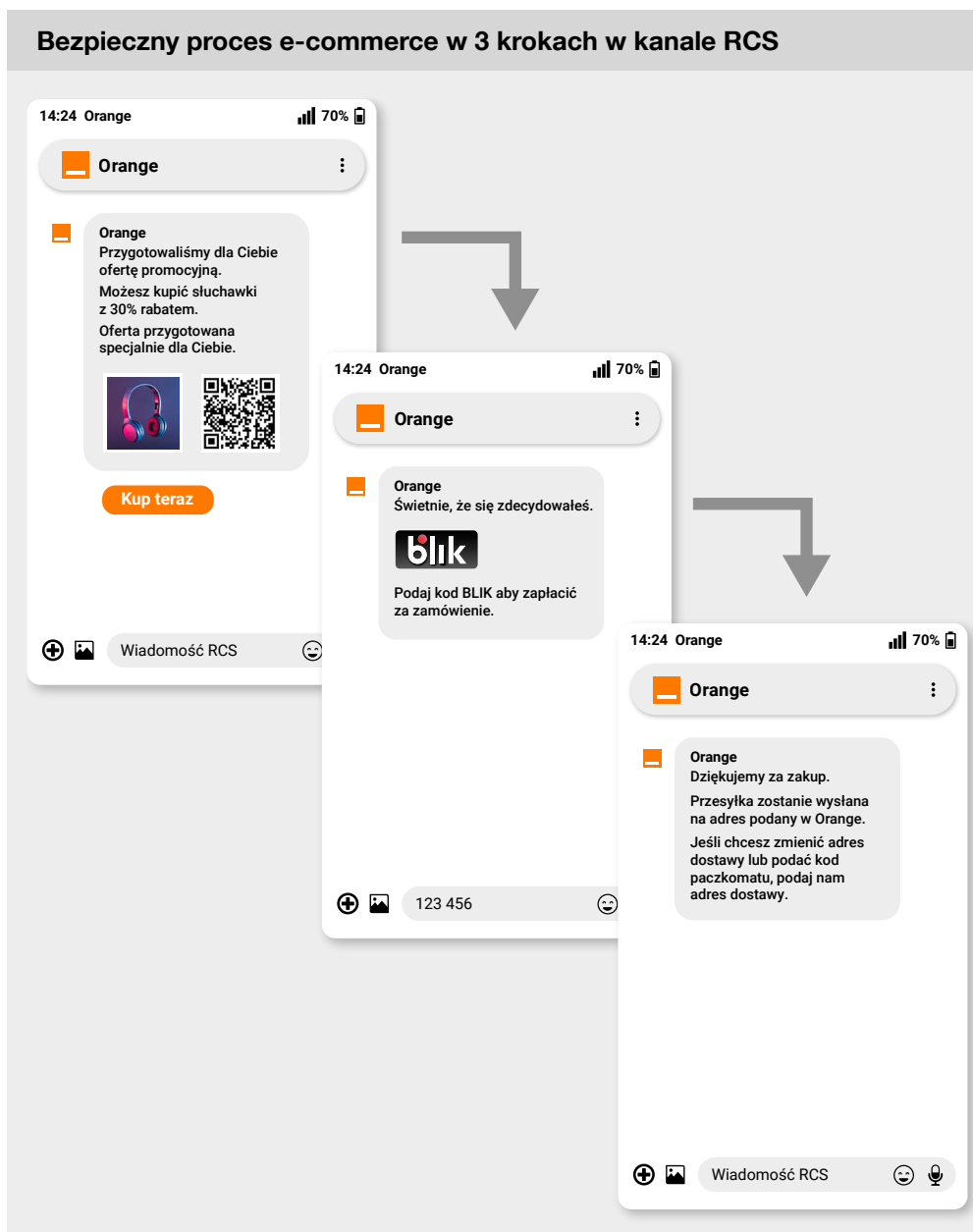


RCS-ie, czy „jesteś lekiem na całe zło”?

Dlatego jeśli planujemy przesłać do naszego odbiorcy informacje reklamowe lub zachęcić do wejścia na stronę WWW, to zrobimy to przez RCS. Oto jak może wyglądać taka wiadomość reklamowa przesłana przez RCS.



RCS umożliwia najbardziej naturalną dla człowieka formę komunikacji, czyli konwersację - wymianę wiadomości w dwie strony. Pozwala to na realizację kompletnego procesu komunikacji w modelu end2end. To doskonałe rozwiązanie m.in. w e-commerce, i to w różnorodnych scenariuszach, np. finalizacji zakupu lub obsługi reklamacji bez konieczności przekierowywania na stronę WWW.



RCS-ie, czy „jesteś lekiem na całe zło”?

CLI Spoofing (ang. **Caller ID Spoofing**), już bez posilkowania się definicjami, to metoda oszustwa, w którym identyfikator dzwoniącego w sieci telefonicznej wskazuje odbiorcy połączenia, że inicjatorem jest stacja inna niż prawdziwa stacja inicjująca. Może to prowadzić do wyświetlenia numeru telefonu innego niż ten, z którego wykonano połączenie. Czy w tym przypadku również możemy wykorzystać RCS do zapobiegania tego rodzaju nadużyciom?

Oczywiście, że tak, a dodatkowo możemy interaktywnie uzgodnić z odbiorcą preferowany czas połączenia. Spójrzmy na taki scenariusz: tradycyjne połączenie przychodzące po kilku próbach nadużyć z tego samego lub różnych numerów jest przez kolejnych użytkowników zgłaszane jako spam. Nawet jeżeli dzwoni zaufana instytucja! W efekcie, skuteczność połączeń telefonicznych drastycznie spada.

W takim przypadku przed połączeniem naszego konsultanta możemy zaanonsować rozmowę certyfikowanym i bezpiecznym komunikatem RCS A2P, w którym prześlemy informację, kto będzie dzwonił, w jakiej sprawie i z jakiego numeru telefonu. Dodatkowo możemy też dać odbiorcy możliwość np. potwierdzenia chęci rozmowy, przełożenia np. 30 min później lub umieścić w wiadomości RCS przycisk akcji umożliwiający oddzwonienie.

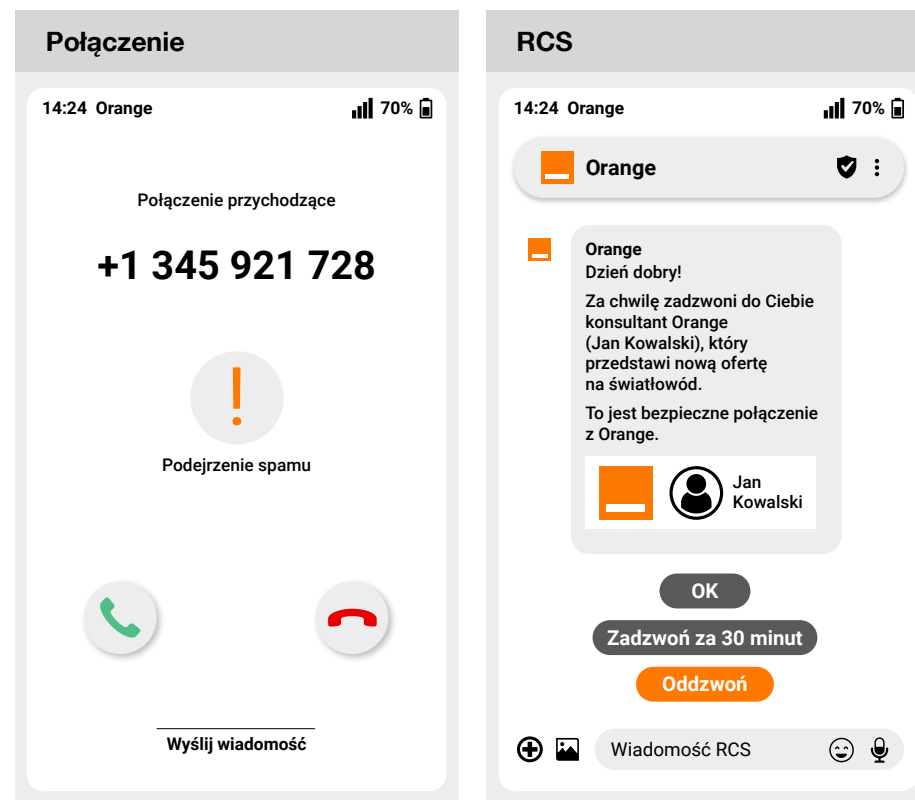
„Oto cały Ty!”

Artykuł ten można byłoby spuentować parafrazą wersu z piosenki Krystyny Prońko: „Oto cały RCS”. Przedstawiliśmy jednak tylko kilka wybranych zastosowań tej technologii, które opisaliśmy w ważnym lecz wąskim kontekście bezpieczeństwa i zaufanego kanału komunikacji. Mamy nadzieję, że przykładowe scenariusze zainspirują Was do pomysłów jak w bezpieczny sposób zastosować kanał RCS w Waszych obszarach: do komunikacji i reklamy Waszych produktów, a nawet w przypadku usług serwisowych, takich jak infolinie czy pomoc doradców w procesie zakupowym.

„I nadzieję na przyszły rok...”

Czy RCS stanie się efektywnym standardem w bezpiecznej komunikacji biznesowej? Wszystko na to wskazuje. Decydująca wydaje się zeszłoroczna decyzja Apple o dostępności RCS na urządzeniach z iOS. Zwiększy to globalny zasięg tej technologii o 1,5 miliarda osób. To prawdziwy przełom, który zrewolucjonizuje i ujednotoczy sposób naszej komunikacji za pomocą smartfonów.

Światowy trend wzrostu komunikacji przez RCS jest również widoczny w polskiej sieci Orange. Codziennie ponad 1,5 tys. nowych użytkowników aktywuje usługę RCS. Szacujemy, że na koniec 2026 roku prawie 9 milionów użytkowników naszej sieci będzie korzystało z tej usługi. Również Orange w komunikacji ze swoimi klientami wykorzystuje aktywnie technologię RCS i zachęca swoich partnerów do używania tego bezpiecznego kanału komunikacji.



Jak budować przewagę biznesową, gdy konkurencja ceną nie jest możliwa?

Studium przypadku



Orange Wholesale jest częścią hurtową **Orange Polska** i zapewnia kompleksowe rozwiązania dla przedsiębiorców telekomunikacyjnych. Operatorzy mogą korzystać m.in. z największej w kraju infrastruktury telekomunikacyjnej, w tym sieci światłowodowej, dostępu do internetu, transmisji danych oraz projektów technicznych. W ramach usługi MVNO, Orange otworzył także swoją sieć mobilną, na bazie której nawet mali i średni operatorzy mogą budować własne telefonie komórkowe.

Dzięki tak komplementarnej ofercie wszystkie elementy niezbędne do budowy i rozwoju biznesu operatorskiego są w jednym miejscu. Dostępne w prosty sposób i na przyjaznych zasadach, w ramach przejrzystej i stabilnej współpracy.

Telestrada specjalizuje się w dostarczaniu zaawansowanych technologicznie rozwiązań telekomunikacyjnych, zarówno dla klientów indywidualnych, jak i biznesowych. W jej portfolio znajdują się m.in. marka **lajt mobile**. **Lajt mobile** to innowacyjna sieć MVNO, która od 2015 roku łączy prostotę z konkurencyjnymi cenami, rewolucjonizując rynek telekomunikacyjny.

Firma oferuje jedno z najtańszych abonamentów, zapewniając niezawodny zasięg i stałe ceny przez cały okres umowy. Wyróżnia się także wyjątkową obsługą klienta – zamiast botów, oferuje bezpośredni kontakt z doradcami, którzy pomagają na każdym etapie współpracy. Dbłość o bezpieczeństwo danych klientów oraz stabilność usług to priorytet marki.

Jak budować przewagę biznesową, gdy konkurencja ceną nie jest możliwa?

Studium przypadku

Wyzwanie

Lajt mobile, podobnie jak wszystkie MVNO, działało w oparciu o zasięg jednej sieci udostępnianej przez dużego operatora. Takie rozwiązanie pozwalało na zbudowanie konkurencyjnej oferty – szczególnie w pierwszych latach działalności – i oferowanie atrakcyjnych cenowo planów komórkowych. Wraz z coraz bardziej dojrzewającym rynkiem i rosnącą konkurencją w segmencie wirtualnych sieci komórkowych, widoczne stały się ograniczenia związane z takim modelem.

Głównymi wyzwaniami były:

- brak możliwości dalszego konkurowania wyłącznie ceną, ponieważ rynek wymaga nowych, innowacyjnych rozwiązań,
- niezadowolenie części klientów z zasięgu sieci,
- potrzeba wyróżnienia się na tle konkurencji, która coraz bardziej różnicowała swoje oferty.



Rozwiązanie

Doświadczenie historyczne Telestrady wskazywało, że optymalnym rozwiązaniem będzie – oprócz odświeżenia oferowanych usług – dywersyfikacja dostawców usług hurtowych. Lajt mobile jako pierwsza wirtualna sieć w Polsce postanowiła pozwolić klientom na wybór sieci, z jakiej chcą korzystać.

Poszukiwania nowego partnera rozpoczęto na przełomie 2021 i 2022 roku. Ostatecznie – po szeregu rozmów i testów – wybór padł na Orange. Głównymi powodami były:

- **szeroki i stabilny zasięg** – Orange oferuje jeden z najlepszych zasięgów w Polsce; dotyczy to także obszarów, gdzie sieć drugiego MNO jest mniej efektywna,
- **innowacyjne podejście technologiczne** – Orange dysponuje nowoczesną infrastrukturą, co przekłada się na jakość połączeń i transmisji danych,
- **pozytywny odbiór wśród klientów końcowych** – Orange cieszy się zaufaniem i dobrą reputacją, co miało znaczenie dla klientów lajt mobile.

Umowę podpisano w czerwcu 2023.

Orange oferuje dwa modele współpracy, związane ze sposobem rozliczeń. Pakietowy – zapewnia stałą cenę za usługi, np. za nielimitowane rozmowy, SMS-y i MMS-y oraz różnej wielkości paczki danych. PAYG (pay-as-you-go) to opcja dla operatorów, którzy mają już doświadczenie na rynku mobilnym i znają potencjał swoich klientów.

Oplata pobierana jest za efektywne zużycie jednostkowe każdej usługi, np. transmisji danych (liczonych w GB), usług głosowych (za minutę połączenia) oraz SMS i MMS (za sztukę).

Lajt mobile zdecydowało się na model PAYG i dostęp do platformy MVNE przez API (Orange oferuje także dostęp bezpośrednio przez przeglądarkę internetową). Platforma jest prostym, funkcjonalnym i bezpiecznym narzędziem, dzięki któremu można:

- zarządzać procesami operacyjnymi swojej wirtualnej sieci,
- prowadzić obsługę swoich klientów,
- zarządzać usługami dodatkowymi dla abonentów,
- kontrolować bilingi klientów.

Proces wdrożenia – od podjęcia decyzji do czasu komercyjnego uruchomienia usługi – trwał około 6 miesięcy. To bardzo szybkie tempo, bowiem na rynku podobne projekty trwają nawet 1,5 roku. Było to możliwe dzięki простemu modelowi MVNO Orange, zrozumiałej dokumentacji oraz partnerskim relacjom. Istotne okazało się także doświadczenie obu stron w zakresie obsługi klienta końcowego i znajomość jego potrzeb. Na każdym etapie wdrażania poszczególnych komponentów Telestrada miała zapewnione techniczne wsparcie Orange.

Jak budować przewagę biznesową, gdy konkurencja ceną nie jest możliwa?

Studium przypadku

Elementy projektu	
lajt mobile	Orange
analiza dokumentacji technicznej dostarczonej przez Orange	wdrożenie lajt mobile w systemach OPL (platforma MVNE, konfiguracja serwera sFTP)
identyfikacja obszarów do zmian technicznych po stronie lajt mobile	integracja API systemów lajt mobile z platformą MVNE
budowa fizycznej komunikacji z platformą MVNE	przeprowadzenie testów API, serwera sFTP, procesów aktywacyjnych i zarządzania kartami SIM (provisioningowych)
integracja systemów lajt mobile z platformą MVNE	produkcja spersonalizowanych kart SIM lajt mobile
przebudowa procesów organizacyjnych, ofertowych i technicznych	
projekt kart SIM lajt mobile	

Przy tak złożonym projekcie, który „szyty jest na miarę” i dostosowywany pod konkretne potrzeby, istotnym elementem jest także bieżąca komunikacja:

- wspólne wypracowywanie rozwiązań uwzględniające techniczne możliwości Orange i lajt mobile,
- niezwłoczne reagowanie na zgłaszane potrzeby oraz uwagi,
- szybkie podejmowanie decyzji.

Wyniki

Dzięki współpracy z Orange, lajt mobile jako pierwsza sieć komórkowa w Polsce umożliwiła klientom wybór między zasięgiem dwóch operatorów – Plus i Orange. W efekcie wyróżniła się na rynku, łącząc innowacyjność z troską o potrzeby klientów i wzmocniła zaufanie do marki oraz jej konkurencyjność.

Decyzja o dywersyfikacji dostawców zasięgu i nawiązaniu współpracy z Orange przyniosła także szereg pozytywnych zmian na poziomie organizacyjnym, jak i biznesowym:

- **poszerzenie bazy klientów** – rozwiązanie przyciągnęło nowych użytkowników, szczególnie tych, którzy wcześniej mieli obawy związane z ograniczeniami zasięgu dotychczasowego operatora w ich lokalizacjach,
- **wzrost przychodów** – zwiększenie zainteresowania usługami lajt mobile, spowodowało wzrost przychodów firmy,
- **optymalizacja organizacyjna** – wdrożenie rozwiązania wymagało usprawnienia procesów wewnętrznych i wprowadzenia narzędzi wspierających obsługę dwóch operatorów zasięgu, co przyczyniło się do wzrostu efektywności działania firmy,
- **zwiększenie konkurencyjności** – innowacyjne podejście wyróżniło lajt mobile na tle konkurencji, umacniając jej pozycję na rynku telekomunikacyjnym,
- **lepsze dopasowanie usług** do indywidualnych potrzeb klientów i warunków lokalnych,
- **poprawę jakości usług**, szczególnie w obszarach, gdzie zasięg pierwotnej sieci był ograniczony,
- **elastyczność przy zachowaniu niskich cen**, co wzmocniło wizerunek marki jako dostawcy przystępnych i dopasowanych rozwiązań,
- **wzrost satysfakcji klientów** – wybór sieci pozwolił dopasowywać usługi do swoich indywidualnych potrzeb.

Jak budować przewagę biznesową, gdy konkurencja ceną nie jest możliwa?

Studium przypadku

Orange z kolei:

- znacząco zwiększyło bazę aktywnych kart SIM i obserwuje jej stały miesięczny wzrost,
- zanotowało istotny wzrost przychodów w segmencie MVNO,
- dzięki współpracy i wprowadzaniu rozwiązań oczekiwanych przez lajt mobile, uatrakcyjniło ofertę (m.in. w zakresie roamingu dla MVNO) i tym samym podniosło jakość świadczonych usług,
- rozwinęło możliwości środowiska testowego i miało możliwość wdrożenia oraz przetestowania nowych produktów, m.in. publiczny adres IP i eSIM,
- dzięki poznaniu potrzeb dużego MVNO i problemów, oferuje jeszcze bardziej elastyczne rozwiązania.

Dlaczego warto zdywersyfikować dostawców MNO

Dywersyfikacja dostawców zasięgu to rozwiązanie, które może przynieść wiele korzyści firmom telekomunikacyjnym, które działają w modelu MVNO. Najważniejsze to:

1. **Skalowalność** – rozwiązanie może być skalowane i adaptowane do różnych segmentów rynku, w zależności od potrzeb klientów i potencjalnych partnerów technologicznych;
2. **Lepsza jakość** – poprawa jakości świadczonych usług, w tym m.in. większy zasięg sieci;
3. **Bezpieczeństwo** – dywersyfikacja zwiększa stabilność biznesu i pozwala uniknąć wielu pułapek, takich jak vendor-lock (np. w przypadku zablokowania przez innego MNO cen);

4. **Elastyczność oferty** – możliwość łatwego przeniesienia bazy klientów do drugiego MNO; umożliwienie wyboru zasięgu pozwala lepiej odpowiadać na potrzeby klientów, co zwiększa ich satysfakcję i przekłada się na lojalność;
5. **Wyróżnienie na rynku** – wprowadzanie innowacyjnych rozwiązań, takich jak wybór operatora zasięgu, pomaga budować przewagę konkurencyjną i przyciągać nowych klientów;
6. **Budowa wizerunku marki** – oferowanie rozwiązań dostosowanych do klientów świadczy o profesjonalizmie i trosce o użytkowników, co buduje pozytywny odbiór firmy.



Jak budować przewagę biznesową, gdy konkurencja ceną nie jest możliwa?

Studium przypadku

Komentarze



Michał Reutt, Dyrektor Marketingu i Rozwoju w Orange Wholesale

Chcemy być dla operatorów MVNO dostawcą rozwiązań pierwszego wyboru. Mamy poważne atuty: doskonałą sieć mobilną, łatwy dostęp do platformy MVNE oraz kompleksową i nowoczesną ofertę zbudowania własnej telefonii komórkowej. Uzupełniają je przyjazne warunki współpracy oraz profesjonalna obsługa zarówno na etapie sprzedaży jak i wdrożenia usługi.

Dywersyfikacja dostawców jest naszym zdaniem jednym z najprostszych, a zarazem niezbędnych etapów rozwoju biznesu w konkurencyjnym środowisku operatorów wirtualnych. Nie myślimy zresztą jedynie o klasycznym MVNO, ale także o rozwoju – we współpracy z operatorami – usług przyszłości.



Anna Ossowska-Osuch, Dyrektor marki lajt mobile

Decyzja o współpracy z Orange była dla nas strategicznym krokiem w kierunku zaspokojenia rosnących potrzeb naszych klientów i dalszego rozwoju marki. Dzięki nowemu modelowi zyskałoby nie tylko możliwość oferowania jednych z najbardziej konkurencyjnych rozwiązań na rynku, ale również szansę na wprowadzenie innowacyjnych usług.

Szczególnie cieszy nas elastyczność, jaką daje model PAYG i dostęp do platformy MVNE przez API. Taki sposób współpracy pozwala nam na precyzyjne dostosowywanie oferty do zmieniających się potrzeb rynku oraz budowanie przewagi konkurencyjnej.

Możliwość wyboru między zasięgiem dwóch operatorów to rozwiązanie, które wyróżnia nas wśród dostawców MVNO w Polsce. Nie tylko zwiększyło to satysfakcję obecnych klientów, ale również przyciągnęło nowych użytkowników, którzy wcześniej mieli wątpliwości co do jakości zasięgu. Dodatkowo, wprowadziliśmy szereg usprawnień organizacyjnych i procesowych, które wzmacniają naszą efektywność operacyjną.

Nasze partnerstwo z Orange to przykład tego, jak współpraca z dużym, doświadczonym operatorem może wspierać dynamiczny rozwój mniejszej marki, jednocześnie zwiększając zaufanie i lojalność klientów.



Słowniczek

MVNO

Mobile Virtual Network Operator (MVNO) to wirtualny operator mobilny. Wykorzystuje infrastrukturę oraz usługi dostarczane przez MNO w jednym z modeli współpracy: Full MVNO (gdy posiada własną sieć szkieletową), Light MVNO (gdy nie posiada własnej sieci szkieletowej), Branded reseller.

MNO

Mobile Network Operator (MNO) to operator infrastrukturalny, który posiada własną sieć szkieletową i radiową, obsługuje użytkowników końcowych, ale może też sprzedawać hurtowo dostęp do swojej sieci.

MVNE

Mobile Virtual Network Enabler (MVNE) oferuje usługi informatyczne strukturalizujące działalność operacyjną MVNO, najczęściej w formie platformy do prowadzenia rozliczeń i zarządzania usługami abonentów.

Partnerzy biorący udział w przygotowaniu raportu

- 24IT Media
- AVIS Mariusz Ziółkowski
- borkow.org PPHU
- Cheeloo J. Turczyn i Wspólnicy Sp. J.
- CHOJNET
- Codeplant Sp. z o. o.
- Dariusz Mierzwa Graficom
- ELTRONIK
- EnergyLux Sp. z o.o.
- E-nernet sp. zo.o.
- E-Punkt Systemy Informatyczne
- Firma Usługowa Delta
- Firma Usługowo Handlowa Krzysztof Zarębski
- Gawex Media sp. z o.o.
- HD.net Daniel Kąciak
- hiperia sp. z o.o.
- INM Sp. z o.o.
- Intelly
- INTERA SP. z o.o.
- KAJA Komputer
- KLIKOM.NET Sp. z o.o.
- Macrosat sp. z o.o.
- MATRIX Cezary Taraszkiewicz
- Mat-Sat Telecom
- Maxnet Łukasz Hamerski
- Media Telekom Sp. z o.o.
- Mediasat sp.j.
- Metrosan sp. z o o
- Microchip
- Mikonet
- Netcom IT S.p. z o.o.
- PSTD Sp. z o.o.
- PT LANET sp. z o.o.
- RWD Prospect Sp. z o.o.
- SACOM SYSTEM
- SOJA-NET
- STARTNET
- STELLA ZIT
- Systemia.pl
- TELGAM
- Tempus
- TVK BORUTA
- YNET MANAGEMENT Paweł Skrodzki



Zespół redakcyjny:

Marcin Kruszyński, Tomasz Łabanowski, Małgorzata Stochmal, Marta Tokarska



Z ORANGE WHOLESale
BIZNES SIĘ KRĘCI!



Wholesale



Infolinia 19 333



hurt-orange.pl