ICT PROFESSIONAL

ISSN 2449-5581

WWW.ICTPROFESSIONAL.PL #32 (WIOSNA 2022)

WRÓG U BRAMEK STR. 10

800+ UCZESTNIKÓW

2.8Tbps+ RUCHU IP

1300+ PORTÓW

Jesteśmy największym IXP w Polsce, opartym na trzech niezależnych węzłach: Katowice, Warszawa i Poznań. Powstaliśmy, aby dbać o interesy i zaspokajać potrzeby polskich MiŚOT-ów, czyli Małych i Średnich Operatorów Telekomunikacyjnych. Przedsięwzięcie to stworzyliśmy i prowadzimy w oparciu o kapitał i pracę polskich, lokalnych ISP. Zyski z działalności przeznaczamy na inwestycje w sprzęt, wzbogacanie zasobów, projekty celowe i integrację środowiska.

Współpraca z nami bazuje na wzajemnym zaufaniu i zadowoleniu, braku korporacyjnych utrudnień, opóźnień oraz niepotrzebnych kosztów. Nigdy nie konkurujemy z ISP na rynku detalicznym czy biznesowym.

W naszych OpenPeeringach, kosztujących już od kilkudziesięciu złotych, oddajemy Wam już znacznie ponad połowę Internetu. Realizujemy bezpośredni dostęp do międzynarodowych operatorów: Arelion (d.Telia), Lumen, Liberty Global, GTT, Hurricane Electric i Telecom Italia Sparkle, w cenach hurtowych. Zapewniamy prosty i tani dostęp do treści pozostałych polskich IX-ów w ramach jednej usługi – Polmix, dokładnie tyle, ile potrzebujesz, bez płacenia za porty i niewykorzystane pasmo. Agregujemy ogólnopolskie zakupy ISP, wolumenu usług międzynarodowych, polskich i transmisji danych – regularnie obniżamy ceny. Posiadając port w EPIX, masz dostęp do wszystkich integratorów IPTV i dostawców innych usług.

WWW.EPIX.NET.PL

IX, W KTÓRYM REGULARNIE SPADAJĄ CENY I TAK W KÓŁKO OD 12 LAT

MiSOT GRUPA

Agresja Rosji na Ukrainę zmieniła współczesną rzeczywistość. Jednakże ataki na rządowe serwery i kampanie fake newsów rozpoczęły się na długo przed konwencjonalnymi działaniami militarnymi. Wojny światowe z definicji dzieją się na wielu frontach. Świat wirtualny też ogarnął konflikt, być może nawet cyberwojna światowa. Dlatego w redakcji ICT Professional uznaliśmy, że temat cyberbezpieczeństwa powinien wybrzmieć na wielu kartach niniejszego numeru.

Destabilizacja państwa we współczesnym świecie możliwa jest nie tylko poprzez walkę na polu bitwy. Równie niebezpieczne skutki może przynieść ingerencja w systemy informatyczne. W przypadku uszkodzenia kluczowych elementów infrastruktury kraju możliwy jest jego całkowity paraliż. Warto wiedzieć, jak się bronić.

Prześledziliśmy najnowsze wydarzenia i trendy w dziedzinie bezpieczeństwa internetu, a eksperci opowiedzieli między innymi o roli krajowego systemu cyberbezpieczeństwa, o tym, co oznacza stan wyjątkowy dla operatorów oraz o destr ukcyjnym wpływie dezinformacji i trollingu. Na łamach ICT Professional Czytelnik przeczyta również historię grupy hakerów Anonymous, dowie się o roli sztucznej inteligencji na polu bitwy i o wpływie działań wojennych na ceny energii w 2022 roku.

Nie zabrakło również tematów lokalnych oraz tych dotyczących przede wszystkim małych i średnich operatorów w Polsce. Wśród przygotowanych artykułów znajdziecie informacje o budowie sieci LoRaWAN (str. 13), o inicjatywie TeleOdpowiedzialni (str. 15) i o TeleCentrum (str. 16), a także garść newsów z innych projektów Grupy MiŚOT: Mapy Dobra w ramach Lokalni.pl (str. 19) i Publikonu (str. 22). W numerze także obszerna fotorelacja z Lokalnego Zjazdu MiŚOT w Janowie Podlaskim (przy okazji zapraszamy na kolejną edycję w Kołobrzegu) oraz raport o działaniach MiŚOT-ów, którzy pomagają uchodźcom z Ukrainy.

Życzymy przyjemnej lektury!

Redakcja ICT Professional i ISPortal.pl

ICT PROFESSIONAL

Kontakt z redakcją
redakcja@ictprofessional.pl

Nr w rejestrze wydawnictw
PR2614

Międzynarodowy znak informacyjny
ISSN 2449-5581

Nakład
3200 egzemplarzy

Redaktor naczelny
Krzysztof Fujarski
tel. +48 600 420 901
krzysztof.fujarski@ictprofessional.pl

Sekretarz redakcji
Michał Koch
michal.koch@misot.pl

Reklama
Bartosz Nowak
tel. +48 602 495 064
bartosz.nowak@misot.pl

Redakcja
Paweł Gniadek, Michał Koch, Marek Nowak, Klaudia Wojciechowska

Skład i grafika
Michał Piechniczek
Grafika na okładce: Marcin Jedynak

Współpraca
Michał Andrzejewski
Paweł Białas
Łukasz Biernacki
Karol Borysow
Tomasz Brol
Magdalena Drozdowska
Marta Heród
Ihor Hreskiv
Maciej Jojczyk
Sebastian Kachel
Paweł Licznar
Maciej Linscheid
Marcin Orocz
Daniel Piecuch
Marcin Pilak
Emil Różański
Krzysztof Zawadzki

Tłumaczenie i korekta
Marlena Fujarska

Wybrane grafiki - Marcin Jedynak, Marcin Łysak, freepik.com

Wydawca
MdM MiŚOT

Projekt MdM Sp. z o.o.
ul. Józefczaka 29/40
41-902 Bytom

Druk
Drukarnia Dan-Pol Zabrze

Projekt ICT Professional #32 (wiosna 2022) wydany w maju 2022 r. realizowany jest pod patronatem Grupy MiŚOT.

Czasopismo bezpłatne dla operatorów telekomunikacyjnych w ramach prenumeraty na stronie www.ictprofessional.pl/prenumerata.

WARTO PRZECZYTAĆ

08

Stowarzyszenie e-Południe do premiera: nie blokujmy rozwoju nowoczesnych technologii

Paweł Gniadek

13

LoRaWAN będzie działać na IPv6

Marek Nowak

20

Miliony dla lokalnych operatorów

Michał Koch

26

Relacja ze Zjazdu MiŚOT w Janowie Podlaskim

Michał Koch, Marek Nowak, Paweł Gniadek

36

Lex Huawei, czyli kto się boi KSC?

Marek Nowak

37

Czy cyberbezpieczeństwo jest pretekstem do centralizacji?

Michał Koch

40

Dezinformacja w sieci

Klaudia Wojciechowska

51

Duże zmiany na polskim rynku paliw i energii

Emil Różański

58

Czy nadchodzi koniec telewizji satelitarnej?

Klaudia Wojciechowska

64

Metawersum. Problemy i korzyści

Michał Koch

xbest.pl | Producent i dystrybutor kabli oraz akcesoriów światłowodowych

Siedziba: 00-807 Warszawa, Al. Jerozolimskie 96 | **Oddział w Rybniku**: 44-200 Rybnik, ul. Św. Józefa 141D
+48 32 239 60 00 & 01 | office@xbest.pl

PING z branży

800 MLN ZŁ WIĘCEJ NA CYBERBEZPIECZEŃSTWO

W dniach 25-27 kwietnia odbył się Europejski Kongres Gospodarczy w Katowicach. Rozmawiano o cyfrowej transformacji i o kosztach, jakie trzeba za nią ponieść. Coraz szybsze procesy transformacji cyfrowej wpływają na biznes, administrację czy życie codzienne. Niestety idzie za tym wzrost cyberzagrożenia. A ochrona przed cyberatakami wymaga przeznaczenia na to sporych pieniędzy. Dlatego zwiększenie funduszy na cyberbezpieczeństwo zadeklarował w trakcie Europejskiego Kongresu Gospodarczego w Katowicach Janusz Cieszyński, pełnomocnik rządu ds. cyberbezpieczeństwa.

Podczas panelu poświęconego digitalizacji zastanawiano się też, czy możemy mówić o dostatecznej digitalizacji polskich przedsiębiorstw. Transformacja cyfrowa to także lepsza konkurencyjność firm. Dzisiaj nie można w nią nie inwestować, bo wiele elementów życia związanych jest ze światem cyfrowym. Firmy, które tego nie rozumieją, przegrywają na rynku.

[źródło: pap-mediaroom.pl]

OBYWATELE UE A KOMPETENCJE CYFROWE

Komisja Europejska wskazuje, że 2021 roku 54 proc. mieszkańców Unii Europejskiej w wieku 16-74 lat posiadało przynajmniej podstawowe umiejętności cyfrowe. Jak wypadają na tym tle Polacy? Polska osiągnęła wynik 43 proc. To sprawia, że lądujemy wśród krajów z najniższym wskaźnikiem kompetencji cyfrowych w populacji, przed Rumunią (28 proc.) i Bułgarią (31 proc). Najwyższy odsetek osób z kompetencjami cyfrowymi odnotowano w Holandii i Finlandii (po 79 proc.), a także w Irlandii (70 proc.). Podstawowe umiejętności cyfrowe odnoszą się do pięciu obszarów: umiejętności korzystania z informacji i danych, umiejętności komunikacji i współpracy, umiejętności tworzenia treści cyfrowych, wiedzy nt. cyberbezpieczeństwa oraz umiejętności rozwiązywania problemów z dziedziny IT. Powyższe zdolności to jedne z kluczowych wyznaczników wydajności w kontekście Dekady Cyfrowej, która określa wizję UE w zakresie transformacji technologicznej. Wyznaczony został cel, aby do 2030 roku 80 proc. obywateli UE w wieku 16-74 lat posiadało przynajmniej podstawowe umiejętności cyfrowe.

[źródło: ec.europa.eu]

CYBERBEZPIECZEŃSTWO FIRM ZAGROŻONE. PRACOWNICY OMIJAJĄ ZABEZPIECZENIA

Chociaż wiele mówi się o cyberzagrożeniach i firmy inwestują w zabezpieczenia przed nimi, to wszystko, jak zwykle, zależy od czynnika ludzkiego. Pracownicy omijają zabezpieczenia chroniące przed cyberprzestępcami, narażając firmy na ataki i straty. Raport Cisco dotyczący świadomości i praktyki cyberbezpieczeństwa wśród osób zatrudnionych w polskich przedsiębiorstwach i organizacjach nie przynosi optymistycznych wieści. Badanie objęło 500 pracowników z małych i średnich przedsiębiorstw (do 500 zatrudnionych) z różnych segmentów gospodarki. W firmach tych stosuje się zdalny lub hybrydowy model pracy. Najpowszechniejszym działaniem jest phishing. Raport Orange z kwietnia 2021 r. wskazuje, że to prawie niemal 40 proc. wszystkich wykrytych w tej sieci zagrożeń. Dlatego nawet najlepsze zabezpieczenia firmowe i wydawane na nie pieniądze nie zapewnią bezpieczeństwa, jeśli nie pójdzie za tym uświadomienie pracowników, jak ważne dla firmy i ich stanowiska pracy jest dbanie o cyberbezpieczeństwo.

[źródło: serwisy.gazetaprawna.pl]

NETIA, ORANGE I PLAY DECYZJĄ UOKIK ZWRÓCĄ KLIENTOM OPŁATY

Urząd Ochrony Konkurencji i Konsumentów poinformował, że Netia, Orange i Play oddadzą klientom opłaty za usługi dodatkowe włączane bez wyraźnej zgody. Reklamacje zostały rozpatrzone pozytywnie. Usługi były włączane bez wyraźnej zgody konsumentów, na których spoczywać obowiązek dezaktywacji ich przed końcem okresu bezpłatnego. „Wiele osób piszących do UOKiK nie było świadomych tego, że muszą to zrobić" – podkreślono. Do aktywacji usług dodatkowych dochodziło zarówno przy zawieraniu umowy, jak i podczas jej przedłużania, i to zarówno podczas rozmowy telefonicznej, przez internet, jak i w salonie. Zgodnie z ustawą włączanie dodatkowo płatnych usług musi odbywać się za wyraźną zgodą abonenta po poinformowaniu go o warunkach aktywacji i możliwości rezygnacji z usługi, by uniknąć opłat. Wyraźna zgoda to stwierdzenie „tak" na propozycje operatora. Nie można o tym mówić w sytuacji, gdy warunki oferty zakładają korzystanie z płatnej usługi jako konieczności przy korzystaniu z warunków promocyjnych umowy z operatorem. „Konsument powinien mieć rzeczywistą możliwość wyboru, a zatem udzielenie odpowiedzi „nie" powinno skutkować brakiem aktywacji danej usługi" – podkreśla urząd. Dlatego decyzją UOKiK Netia, Orange i Play muszą zmienić praktyki, a także zrekompensować konsumentom poniesione straty. Mają zostać wdrożone procedury, w których konsument będzie pytany na etapie zawarcia umowy o zgodę na aktywację dodatkowo płatnych usług. Decyzje urzędu dotyczą obecnych i byłych abonentów. Już teraz te dotyczące Netii i Orange są prawomocne. Na uprawomocnienie decyzji wobec P4 – operatora Play – trzeba jeszcze poczekać.

[źródło: finanse.wp.pl]

ROAMING NADAL BEZ OPŁAT W UE

W lutym 2021 r. KE zaproponowała przedłużenie RLAH, czyli zasad roamingu w UE, które pozwalają na swobodę korzystania z posiadanego abonamentu bez dodatkowych opłat w całej Unii. 13 kwietnia 2022 r. opublikowano odpowiednie rozporządzenie. Oznacza to korzystanie z połączeń mobilnych bez dodatkowych opłat do 2032 r. Opłaty roamingowe w Unii Europejskiej były obniżane od 2006 r., a odpowiednie rozporządzenia (531/2012, 2015/2120, 2017/920) umożliwiły wyjątkową sytuację na skalę świata. W krajach UE oraz Norwegii, Islandii i Liechtensteinie można było korzystać z połączeń telefonicznych i internetowych według stawek krajowych. Użytkownicy nie ponosili z tego tytułu żadnych dodatkowych opłat. Dla operatorów oznaczało to zniesienie detalicznych opłat roamingowych, a w przypadku opłat roamingowych hurtowych wprowadzono pułapy cenowe.

13 kwietnia 2022 r. w Dzienniku Urzędowym UE opublikowany został tekst rozporządzenia roamingowego – Rozporządzenie PE i Rady UE 2022/612 z dnia 06.04.2022 r., które uwzględnia tę propozycję. Oznacza to przedłużenie obecnie obowiązującej sytuacji do końca czerwca 2032 r.

Znowelizowane przepisy wchodzą w życie 1 lipca 2022 r.

[źródło: uke.gov.pl]

W BIELSKU-BIAŁEJ PIENIĄDZE Z NIEZREALIZOWANYCH PROJEKTÓW CYFROWYCH WYKORZYSTAJĄ NA CYBERBEZPIECZEŃSTWO

W Bielsku-Białej zrezygnowano z dwóch projektów cyfrowych. Jednym z nich jest aplikacja mobilna z bieżącymi informacjami. Drugim strona internetowa ze zdigitalizowanymi trasami turystycznymi miasta. Pozwoli to na zaoszczędzenie pieniędzy na zapewnienie cyberbezpieczeństwa infrastrukturze sieciowej w Urzędzie Miejskim. Projekt digitalizacji tras turystycznych pod nazwą „Zwiedzaj Bielsko-Biała online" miał kosztować 50 tys. zł. Taką kwotę na jego cel zabezpieczono w budżecie miasta. Stworzenie miejskiej aplikacji mobilnej z informacjami dotyczącymi miasta wyceniono było na 70 tys. zł. Oba te projekty nie powstaną. Aplikacja miejska dublowała informacje, które znajdują się na innych stronach, dlatego uznano, że jej powstanie nie jest konieczne. Nie wiadomo, jaki był powód rezygnacji z digitalizacji tras turystycznych. Zaoszczędzone w ten sposób pieniądze zostaną wykorzystane na modernizację sieci bezprzewodowej w bielskim magistracie. Pozwoli to na podniesienie poziomu cyberbezpieczeństwa infrastruktury. Przy okazji zapewniono też sprawne środowisko dla urządzeń przenośnych i podłączenie do sieci Wi-Fi.

[źródło: bielsko.biala.pl]

ZGODNIE Z DECYZJĄ UE BĘDZIE JEDNA ŁADOWARKA. CO TO OZNACZA DLA PRODUCENTÓW SPRZĘTU?

Parlament Europejski podjął decyzję ograniczającą ilość elektrośmieci. Gniazdo USB-C będzie obowiązkowym standardem ładowania nie tylko w smartfonach, ale również w tabletach, słuchawkach, padach czy czytnikach e-booków. Rozwiązanie ma być stosowane na terenie całej UE. Komisja Rynku Wewnętrznego i Ochrony Konsumentów PE przegłosowała poprawkę do dyrektywy ujednolicającej standard ładowania. Obowiązującym standardem w smartfonach, tabletach, słuchawkach, padach, sterownikach do konsol wideo, czytnikach e-booków i cyfrowych aparatach ma być USB-C. Z tego standardu będą wyłączone jedynie niewielkie urządzenia, takie jak smartwatche czy sprzęt, w którym inne porty używane są ze względów bezpieczeństwa (np. szczoteczki elektryczne). Przepisy miałyby obowiązywać od 2026 r.

[źródło: cyfrowa.rp.pl]

CYFRYZACJA UKRAINY TAJEMNICĄ JEJ SUKCESU

Wojna w Ukrainie pokazała, jak ważny w obecnych czasach jest rozwój cyfrowy, nawet w tak trudnych chwilach. Digitalizacja Ukrainy rozpoczęła się w 2015 roku. Dzisiaj kraj ten walczy nie tylko na swoim terenie, ale również w cyberprzestrzeni. Bombardowanie infrastruktury, miliony uchodźców, a system wciąż nie upada. Nawet zawieszenie działalności banków zaraz po ataku trwało jedynie kilkanaście godzin. Pieniądze można wypłacać na poczcie, w bankomatach, w sklepach spożywczych, można nadawać paczki, robić zakupy i przelewy. Po każdym ataku, jeśli tylko nie zniszczono całej infrastruktury, bardzo szybko wraca w miarę normalne funkcjonowanie.

Problemem mogło być jednak zagrożenie łączności w trakcie wojny. Dla zdigitalizowanego państwa byłaby to spora przeszkoda. W ramach walki ukraińscy operatorzy sieci komórkowych zdecydowali się na stworzenie wewnętrznego roamingu. Poza tym nie uzależniają oni dostępności usługi od opłacania rachunków. Porozumienie z zagranicznymi operatorami pozwoliło także na wsparcie osób uciekających za granicę – otrzymują one bezpłatne SMS-y, sto minut rozmów i 55 GB internetu za darmo.

[źródło: krytykapolityczna.pl]

LEON ZNOWU Z DIAMENTEM

Leon, operator regionalny na terenie dawnego Rybnickiego Okręgu Węglowego, po raz kolejny uzyskał tytuł Diamentu Forbesa. Prestiżowa nagroda to znaczne wyróżnienie dla firmy, która uczyniła lokalność jednym z atutów. Nagrodę w kategorii przedsiębiorstw o poziomie przychodów do 50 mln PLN odebrał Piotr Majcher, wiceprezes spółki Leon Telekom. – Firmy z rankingu Diamentów Forbesa mogą być wzorem do naśladowania. To firmy absolutnie transparentne i uczciwe, które pokazały, że w trudnych czasach ciągle potrafią rozwijać się w sposób dynamiczny – gratulował Paweł Zielewski, redaktor naczelny magazynu Forbes. W rozmowie z ISPortal.pl Grzegorz Goik, prezes zarządu Leona, wspominał, że firma prowadzi działania na podstawie długofalowego planu, wierząc, że to model biznesowy, który zapewni sukces na rynku. – Nasza filozofia jest taka, żeby od początku inwestować w firmę i robić to bardzo konsekwentnie i rozważnie. Myślę, że po tylu latach możemy powiedzieć, że taka strategia przyniosła bardzo dobre efekty – podsumowuje sukcesy firmy Goik.

[źródło: leon.pl]

WEZWANIA UKE, INTERWENCJA KIKE I STOWARZYSZENIA E-POŁUDNIE

Krajowa Izba Komunikacji Ethernetowej oraz Stowarzyszenie e-Południe podjęły interwencję u Prezesa Urzędu Komunikacji Elektronicznej w sprawie przekazania przez operatorów informacji odnoszących się do posiadanej przez nich infrastruktury telekomunikacyjnej. Przypomnijmy, że operatorzy wezwani zostali przez Prezesa Urzędu Komunikacji Elektronicznej do przekazania danych związanych z posiadaną infrastrukturą telekomunikacyjną. Ich wątpliwości wzbudził sposób przekazywania tych danych, wielu sygnalizowało także trudności we wprowadzaniu danych do formularza. Zainterweniowały organizacje branżowe. Przesłane do UKE stanowisko KIKE zostało udostępnione na stronie izby:

NOWE PRZEWIDYWANIA INTELA MÓWIĄ O KRYZYSIE RYNKU PÓŁPRZEWODNIKÓW DO 2024 R.

W swoich poprzednich prognozach Intel mówił o problemach z dostawami półprzewodników do 2023 r. Teraz okazuje się, że te przewidywania były zbyt optymistyczne. W najnowszych prognozach firma podaje już rok 2024. Kryzys dotyczy branży komputerowej, ale też całego RTV/AGD i segmentu samochodowego. W wywiadzie dla CNBC Pat Gelsinger, dyrektor generalny Intela, zweryfikował swoje wcześniejsze przewidywania dotyczące kryzysu na rynku półprzewodników i obecnie datą jego zakończenia ma być nie 2023, a 2024 rok. Spowodowane jest to problemami w łańcuchu dostaw maszyn niezbędnych do produkcji półprzewodników i wpływa to na powstawanie fabryk produkujących półprzewodniki. Firmy starają się przeciwdziałać kryzysowi – Intel modernizuje i buduje nowy kompleks w USA. Rozbudowuje też swoją sieć w Europie, gdzie powstanie nawet nowa fabryka.

To z kolei zwiększa popyt na specjalistyczne maszyny produkcyjne, z którymi też są problemy. Tak zamyka się koło i przedłuża kryzys.

[źródło: dobreprogramy.pl]

POLSKA PRZEGRAŁA W TSUE. PLATFORMY CYFROWE MUSZĄ WERYFIKOWAĆ TREŚCI UŻYTKOWNIKÓW

Trybunał Sprawiedliwości UE oddalił skargę wniesioną przez Polskę. Oznacza to konieczność weryfikacji przez platformy cyfrowe treści od użytkowników. Polska wniosła skargę na art. 17 dyrektywy w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym. Uznała przepis za naruszający wolność wypowiedzi i informacji zagwarantowaną przez Kartę praw podstawowych Unii Europejskiej. Nakazuje on weryfikację treści przesłanych przez użytkowników przez platformy cyfrowe. Zgodnie z art. 17 dostawcy usług udostępniania treści online są odpowiedzialni za bezprawne umieszczenie różnych treści objętych ochroną. TSUE ogłosił wyrok w sprawie polskiej skargi i ją oddalił. Zwrócił uwagę na fakt, że mając świadomość zagrożeń, jakie mogą przynieść narzędzia automatycznego rozpoznawania i filtrowania, ustanowiono jasne granice dla takich środków. Jednocześnie dostosowując art. 17 do prawa wewnętrznego, państwa członkowskie – w tym Polska – mają opierać się na wykładni przepisu pozwalającej zapewnić sprawiedliwą równowagę między prawami podstawowymi chronionymi przez kartę praw podstawowych.

[źródło: wirtualnemedia.pl]

KODEKS DOBRYCH PRAKTYK W ZAKRESIE DEZINFORMACJI

Dezinformacja w internecie staje się coraz bardziej powszechna. Ma to głównie związek z trwającą w Ukrainie wojną. Dlatego też powstał Kodeks Dobrych Praktyk w zakresie dezinformacji, który zawiera kluczowe zagadnienia dotyczące walki z dezinformacją oraz rekomendowane działania.

Kodeks powstał we współpracy ekspertów Crazy Nauki, CyberDefence24, FakeHunter, Instytutu Zamenhofa, Fundacji Rozwoju Przez Całe Życie, Fundacji Nauka. To Lubię, Spider's Web+, Stowarzyszenia Demagog, Stowarzyszenia Pravda, Stowarzyszenia Sieć Obywatelska Watchdog Polska i NASK-PIB. Kodeks Dobrych Praktyk w zakresie dezinformacji ma pomóc zrozumieć procesy dezinformacyjne zachodzące w polskiej infosferze. Pokazuje ich charakterystykę, a także sposoby na przeciwdziałanie takim technikom.

Kodeks Dobrych Praktyk w zakresie walki można pobrać ze strony NASK.

[źródło: biuro prasowe NASK]

STOWARZYSZENIE e-POŁUDNIE DO PREMIERA: NIE BLOKUJMY ROZWOJU NOWOCZESNYCH TECHNOLOGII

PAWEŁ GNIADEK

Stowarzyszenie e-Południe, w imieniu członków i współpracujących operatorów, skierowało list do premiera i ministra cyfryzacji Mateusza Morawieckiego. W piśmie zwrócono uwagę na fakt, że grudniowy projekt zmian w ustawie Prawo komunikacji elektronicznej może ograniczyć rozwój technologii LoRaWAN w Polsce.

Stowarzyszenie podkreśla w liście, że w grudniowej wersji PKE ujęto zmiany, które wprowadzają nowe obowiązki, niewykonalne w przypadku urządzeń działających w technologiach LoRaWAN czy Sigfox.

„Zmiany w projektowanych art. 43 i 45 PKE są niepokojące, ponieważ wymagają tego, aby w przypadku każdej technologii możliwe było ustalenie lokalizacji urządzenia niezależnie od tego, czy zostało wykonane połączenie. Tymczasem technologie LoRaWAN czy Sigfox nie pozwalają na ustalenie lokalizacji urządzenia w przypadku, gdy urządzenie to nie ma aktywnego połączenia" – czytamy w liście do premiera.

M2M na początku drogi

Nowoczesne technologie, takie jak LoRaWAN czy Sigfox, ze względu na swoją specyfikę służą przede wszystkim zapewnieniu komunikacji maszyna–maszyna, w tym także łączności z urządzeniami, których lokalizacja nie jest stała. Aplikacje wykorzystujące komunikację maszyna–maszyna (M2M) są na rynku polskim w początkowej fazie popularyzacji.

– W imieniu Stowarzyszenia e-Południe zaapelowaliśmy do premiera o powstrzymanie się od wprowadzania do projektu PKE regulacji, które mogą doprowadzić do zahamowania rozwoju nowoczesnych technologii – informuje Adam Kossowski, prezes Stowarzyszenia e-Południe.

Mali i średni operatorzy telekomunikacyjni od lat stosują najbardziej nowoczesne i innowacyjne technologie.

Rozwój LoRaWAN

– Jedną z technologii, którą MiŚOT-y już wspólnie wykorzystują i pragną rozwijać, jest LoRaWAN. Popularność jej stale rośnie, zarówno w Polsce, jak i na całym świecie. Komunikacja w technologii LoRaWAN służy do bezprzewodowego przesyłania niewielkich pakietów danych na stosunkowo duże odległości. Sieć LoRaWAN może być atrakcyjnym sposobem zapewnienia taniej komunikacji maszyna–maszyna, ponieważ w tym wypadku niejednokrotnie nie ma potrzeby przesyłania dużych pakietów danych i zapewniania łączności szerokopasmowej – tłumaczy Krzysztof Czuszek, wiceprezes Stowarzyszenia e-Południe.

Komunikacja maszyna–maszyna może mieć kluczowe znaczenie dla rozwoju nowoczesnej gospodarki w Polsce. Standard LoRaWAN jest wspierany i promowany przez globalne stowarzyszenie LoRa Alliance. Do stowarzyszenia należą m.in. Cisco, Orange, IBM, jak również Projekt MdI (MiŚOT dla Internetu rzeczy). Międzynarodowy Związek Telekomunikacyjny (ITU) oficjalnie uznaje LoRaWAN za standard komunikacyjny dla LPWAN (ang. low power wide area network, czyli sieć rozległa małej mocy).

Nowa technologia wymaga regulacji

Łączność maszyna–maszyna, w tym zapewniana dzięki technologii LoRaWAN, ma być regulowana przepisami PKE. Niestety niektóre zmiany wprowadzone do grudniowego projektu ustawy nie uwzględniają specyfiki technologii.

Do projektu aktu prawnego dodano – jak czytamy w uzasadnieniu – „obowiązek udostępniania uprawnionym podmiotom danych lokalizacyjnych powstających lub transmitowanych w sieci telekomunikacyjnej innego przedsiębiorcy telekomunikacyjnego w ra-

mach roamingu krajowego oraz posiadanych przez nich danych o lokalizacji, w sposób zapewniający bieżącą i aktualną lokalizację urządzenia na terytorium Rzeczypospolitej Polskiej, bez względu na technologię świadczonej usługi, co zapewni pełniejsze wykonywanie zadań przez uprawnione podmioty. Proponowana zmiana umożliwi uzyskiwanie przez podmioty uprawnione podczas realizacji kontroli operacyjnej danych lokalizacyjnych urządzenia końcowego, które działa w sieci innego przedsiębiorcy w ramach roamingu krajowego oraz zapewni dostęp do aktualnej lokalizacji niezależnie od tego, czy zostało wykonane połączenie".

Technologia LoRaWAN może służyć zarówno zapewnieniu łączności z urządzeniami znajdującymi się w stałej lokalizacji, umożliwiając np. zdalny odczyt liczników energii elektrycznej, jak i z urządzeniami przemieszczającymi się, optymalizując np. zarządzanie flotą samochodów. W tym ostatnim przypadku podmiot świadczący usługę komunikacji elektronicznej może przetwarzać dane o lokalizacji w rozumieniu PKE. Technologia LoRaWAN nie zapewnia jednak dostępu do aktualnej lokalizacji urządzenia, które w danym momencie nie łączy się z siecią LoRaWAN. Wykonanie nowego obowiązku jest zatem niemożliwe.

Apel o przywrócenie przepisów

– Zaproponowaliśmy przywrócenie brzmienia projektu PKE z września 2021 roku. Chcemy, by obowiązkowi udostępniania uprawnionym podmiotom danych lokalizacyjnych powstających lub transmitowanych w sieci telekomunikacyjnej nie podlegali przedsiębiorcy telekomunikacyjni świadczący usługi komunikacji maszyna–maszyna lub którzy w ramach świadczonej publicznie dostępnej usługi telekomunikacyjnej nie przesyłają komunikatów elektronicznych lub danych związanych z tymi komunikatami – informuje Sebastian Kachel, wiceprezes Stowarzyszenia e-Południe.

Komunikacja maszyna–maszyna może otworzyć wiele nowych obszarów rozwoju dla polskiej gospodarki. Ważne, że przedstawiciele polskich operatorów telekomunikacyjnych, inwestujących w nowoczesne rozwiązania i technologie, zaapelowali do premiera o uwzględnienie w przepisach PKE specyfiki LoRaWAN i zadeklarowali chęć udziału w spotkaniach roboczych, które pozwoliłyby stworzyć regulacje odpowiadające rzeczywistości. ■

Mali i średni operatorzy telekomunikacyjni od lat stosują najbardziej nowoczesne i innowacyjne technologie

e-POŁUDNIE STOWARZYSZENIE

KIKE WSPIERA BUDOWĘ LoRaWAN

KAROL BORYSOW

We wsparcie budowy polskiej sieci LoRaWAN zaangażuje się Krajowa Izba Komunikacji Ethernetowej. Może się to przełożyć na poważne dotacje z programu Fundusze Europejskie dla Nowoczesnej Gospodarki.

Grupa MiŚOT już w 2021 roku rozpoczęła projekt, którego celem jest budowa ogólnopolskiej sieci LoRaWAN (skrót od: Long Range WAN) we współpracy z małymi i średnimi operatorami telekomunikacyjnymi.

– Podczas Lokalnego Zjazdu MiŚOT w Janowie Podlaskim złożyłem deklarację, że izba będzie wspierać ten projekt – mówi Karol Skupień, prezes KIKE. – Jesteśmy też obecnie zaangażowani w prace komisji, która ma zdecydować o szczegółowym brzmieniu przepisów dotyczących przeznaczenia środków FENG. Część z nich ma wspierać badania i rozwój projektów związanych z internetem rzeczy. Jestem przekonany, że budowa polskiej sieci LoRaWAN ma szansę na skorzystanie z nich.

Przypomnijmy, że nadajniki z Grupy MiŚOT zostały już wysłane do operatorów we wszystkich województwach, a w 2022 roku urządzenia trafić mają do wszystkich zweryfikowanych technicznie podmiotów, których przedstawiciele zgłosili akces do projektu Polska LoRaWAN w każdym powiecie. Głównymi plusami tej technologii jest niewielki koszt związany z niskim zużyciem prądu oraz możliwość pozyskiwania informacji z czujników na bardzo duże odległości.

Krzysztof Czuszek z Grupy MiŚOT ocenia, że mali i średni operatorzy telekomunikacyjni mają szansę na co najmniej 20 proc. rynku LoRaWAN w Polsce. Jako jedno z pierwszych komercyjnych wdrożeń tej technologii wskazał monitorowanie pojazdów i towarów na zlecenie korporacji transportowych. ■

WRÓG U BRAMEK

MAREK NOWAK
REDAKTOR NACZELNY ISPORTAL.PL

Tocząca się za naszą wschodnią granicą wojna ma także pośredni wpływ na działania małych i średnich operatorów telekomunikacyjnych działających w Polsce. Dotykają ich głównie zmagania toczące się w cyberprzestrzeni, jednak zasadne jest także, by na przykładzie Ukrainy przyjrzeć się kwestiom związanym z bezpieczeństwem infrastruktury.

Już w pierwszych dniach po rozpoczęciu rosyjskiej inwazji Jurij Szihol, szef Państwowej Służby Łączności Specjalnej i Ochrony Informacji Ukrainy (SSSCIP), stwierdził, że wojna ta jest jednocześnie pierwszą cyberwojną w historii ludzkości. Trudno się z tym nie zgodzić, biorąc pod uwagę liczbę ataków hakerskich odnotowywanych od momentu jej wybuchu. Jest też oczywiste, że bardzo dużo działań dotyczących obronności realizowanych jest przez internet.

Krajobraz przed bitwą

Krajobraz sieciowy Ukrainy przed wojną zbliżony był do tego, jaki znamy w Polsce. Intensywny rozwój usług internetowych w latach 90. odbywał się rękami prywatnych, lokalnych operatorów. Świadczyli oni usługi dostępu do sieci, zanim pojawili się operatorzy korporacyjni. Roczne przychody rynku telekomunikacyjnego zwiększały się z roku na rok (w 2018 roku odnotowano 62 mld hrywien przychodu, co było skokiem aż o 10,2 proc. w odniesieniu do poprzedniego). Najważniejsze węzły wymiany ruchu znajdują się obecnie w Kijowie (UA-IX, DTEL-IX, DataIX), w Charkowie (KH-IX) oraz w Odessie (OD-IX).

Stopniowo też malał koszt dostępu do internetu dla użytkowników końcowych. Ukraina jest obecnie państwem o rozsądnych warunkach dostępu do cyberprzestrzeni, a liczba użytkowników sieci w 2021 roku wyniosła ok. 30 mln osób. Telekomunikacja odegrała też – podobnie jak w Polsce – ważną rolę w czasie trwania pandemii koronawirusa, między innymi w zakresie zdalnego nauczania, co okazało się niezwykle istotne także w czasie wojny.

Protokół kryzysu

Pierwsze informacje z ukraińskiego cyberfrontu nie były jednak optymistyczne. Jeszcze w lutym, kilka dni po rosyjskiej inwazji, Mychajło Fedorow, ukraiński minister transformacji cyfrowej, napisał na Twitterze, że istnieje realna możliwość odcięcia kraju od internetu. Polityk zaapelował jednocześnie do Elona Muska, właściciela SpaceX, o dostarczenie satelitarnego internetu Starlink. Miliarder zgodził się i od tego czasu do Ukrainy docierają kolejne dostawy stacji bazowych Starlink, a ukraińscy dowódcy zachwalają możliwości i wydajność systemu. Musk przestrzegł jednak, że używanie Starlinka może prowadzić do namierzenia użytkowników, więc niezbędne jest korzystanie z niego z rozwagą oraz rozmieszczenie stacji bazowych daleko od skupisk ludzi.

W praktyce okazało się też, że rozproszone sieci ethernetowe są odporniejsze na zniszczenia i łatwiejsze w utrzymaniu. Dziś w większości ukraińskich miast nadal można wypłacać pieniądze z bankomatów, płacić kartą w sklepach spożywczych, nadawać paczki, robić zakupy i przelewy. Po każdym ataku, jeśli tylko nie zniszczono kluczowej infrastruktury, bardzo szybko wraca w miarę normalne funkcjonowanie.

– Pierwsze, co przychodzi mi na myśl w kontekście mobilizacji i wojny w Ukrainie, to ogromna przewaga lokalnych operatorów nad scentralizowanymi firmami – mówi Karol Skupień, prezes KIKE. – Nie padną nam przecież żadne centralne serwery, bo mamy własne, położone nieraz w tej samej miejscowości, w której świadczymy usługi. Kontakt, przynajmniej w ramach społeczności, zostanie utrzymany.

Zespoły techników pracujące w małych i średnich przedsiębiorstwach telekomunikacyjnych są też często doświadczone w utrzymywaniu łączności za pomocą różnych technologii. Światłowody, sieć radiowa, a także łączność na falach krótkich właściwie nie mają przed nimi tajemnic. Technicy przyzwyczajeni są także do reżimu pracy ciągłej i, co chyba najważniejsze, czują się odpowiedzialni za miejscowość, w której żyją. Z drugiej strony zaś duże sieci coraz częściej outsourcingują usługi naprawcze i nie zatrudniają własnych zespołów technicznych.

Cyberwojna

Dzięki obecności wielu podmiotów świadczących usługi dostępu do sieci oraz wsparciu płynącemu z Krzemowej Doliny łączność i możliwość kontaktu ze światem wydaje się w Ukrainie niezagrożona. Kolejnym wyzwaniem jest odpieranie działań destabilizujących ukraińską cyberprzestrzeń. Rosyjscy hakerzy

regularnie atakują strony instytucji państwowych i finansowych, a portale informacyjne zaczęły być zalewane fake newsami.

Zdaniem przedstawicieli strony ukraińskiej w dużej części są to również hakerzy wojskowi, opłacani przez Kreml.

– To ludzie, którzy służą lub pracują na rzecz GRU, Sztabu Generalnego Wojsk Lądowych, FSB i innych instytucji. Posiadają stopnie wojskowe i wykorzystują dane rosyjskiego wywiadu, którymi najprawdopodobniej dzielą się ze zwykłymi cyberprzestępcami – twierdzi Wiktor Żora, wiceszef SSSCIP.

Dzienny rekord to 271 ataków DDoS (ang. Distributed Denial of Service, czyli rozproszona odmowa usługi), polegających na uniemożliwieniu działania sieci poprzez zajęcie wszystkich wolnych zasobów. Ataki te przeprowadzane były równocześnie z wielu komputerów, a ich siła przekraczała nawet 100 Gb/s.

28 marca miał też miejsce największy dotąd cyberatak na Ukrainę. Zaatakowana została infrastruktura IT Ukrtelecom.

Na szczęście wiele cyberataków podejmowanych przez stronę rosyjską jest nieskutecznych lub odpieranych przez zabezpieczenia i działania specjalistów. Udaje się to dzięki zjednoczeniu wokół SSSCIP najlepszych informatyków i specjalistów od cyberbezpieczeństwa.

Wsparcie

W tym zakresie Ukrainę wspiera DIGITALEUROPE oraz jedenaście innych stowarzyszeń branży teleinformatycznej z Europy Środkowej i Wschodniej (także z Polski).

– Reprezentując 36 000 firm zajmujących się cyfryzacją w Europie, od zielonych technologii po dostawców usług opieki zdrowotnej i cyberbezpieczeństwa, wyrażamy naszą pełną solidarność z narodem ukraińskim w obliczu obecnej rosyjskiej agresji – czytamy we wspólnym oświadczeniu organizacji.

W pomoc zaaggażowała się także Grupa MiŚOT.

– Wspieramy działające w Drohobyczu stowarzyszenie zrzeszające małych ukraińskich operatorów telekomunikacyjnych INAU – mówi Marcin Orocz, koordynator transportu Grupy MiŚOT w ramach akcji pomocy Ukrainie. – Ze strony ukraińskiej zbieraliśmy informacje o bieżących potrzebach, a związani z Grupą MiŚOT lokalni operatorzy deklarowali, jaki sprzęt mogą przekazać.

Sprzęt został przekazany przez firmy Syrion, Systel i MCI Tychy.

Na naszym podwórku

Reperkusje cyberwojny dostrzegamy też w naszym kraju. Cyberataki stały się codziennością, a social media stały się przestrzenią, w której trolle internetowe walczą o zasięgi, by szerzyć rosyjską propagandę. Ma to destabilizować sytuację w Polsce i wzbudzić nastroje, które zatrzymają pomoc oferowaną uchodźcom i walczącej Ukrainie.

– Odnotowujemy obecnie setki razy więcej cyberataków niż wcześniej – mówi Marcin Zemła z projektu MiŚOT dla Security. – W skali kraju liczba ta sięga milionów dziennie. Atakowane są serwery pocztowe, dochodzi do brutalnego łamania haseł. Administracja państwowa wprowadziła stałe, stacjonarne dyżury administratorów odpowiedzialnych za kluczowe systemy oraz podniosła poziom kryptografii. Podobne działania zalecałbym każdej firmie telekomunikacyjnej. Ponadto warto sprawdzić i przećwiczyć wszelkie procedury awaryjne. Można też, stosunkowo łatwo, wyłączyć geolokalizację z Rosji i Białorusi, co utrudni (choć nie uniemożliwi) prowadzenie ataków – dodaje.

Szczególne obowiązki związane z raportowaniem incydentów związanych z cyberbezpieczeństwem mają też operatorzy usług kluczowych. Choć operatorzy lokalni nie mają takiego statusu, posiada go EPIX, będący obecnie jedynym polskim i zarazem największym w kraju węzłem wymiany ruchu internetowego. W związku z tym przedstawiciel Stowarzyszenia e-Południe stale przekazuje służbom informacje na temat incydentów, które powodują lub mogłyby spowodować poważne obniżenie jakości lub przerwanie ciągłości działania świadczonej usługi.

– Na przykładzie Ukrainy możemy dziś stwierdzić, że gdyby nie mali i średni operatorzy telekomunikacyjni oraz wsparcie ze strony Elona Muska, dostęp do internetu, a co za tym idzie do informacji, byłby niezwykle ograniczony – konkluduje Marcin Zemła. ■

W praktyce okazało się też, że rozproszone sieci ethernetowe są odporniejsze na zniszczenie i łatwiejsze do utrzymania.

FORMALNA DROGA DO UDOSTĘPNIENIA AKCJI MiŚOT SA OTWARTA

PAWEŁ GNIADEK

11 maja sąd zarejestrował zmiany w statucie MiŚOT SA. Otwiera to formalną drogę do udostępnienia akcji małym i średnim operatorom telekomunikacyjnym, którzy docelowo obejmą do 61 proc. akcji spółki. Wkrótce do MiŚOT-ów trafią listy intencyjne ze wzorem deklaracji przystąpienia do spółki. Pozwoli to na zbudowanie tak zwanej księgi popytu.

– Rok temu rozpoczęliśmy budowę stabilnej i wiarygodnej dla rynku Grupy MiŚOT, która czerpie z dorobku Stowarzyszenia e-Południe. Naszym celem jest skuteczna i efektywna działalność na rzecz MiŚOT-ów, czyli dostarczanie konkurencyjnych cenowo produktów i usług. Najważniejsze jednak, że spółka będzie należeć i pracować dla operatorów. Po decyzji sądu przyspieszamy z formalnościami. Wreszcie możemy realizować nasze zobowiązania, które podjęliśmy wobec środowiska – mówi Krzysztof Czuszek, wiceprezes Stowarzyszenia e-Południe i jednocześnie wiceprezes MiŚOT SA.

Na pierwszym Lokalnym Zjeździe MiŚOT w Bukowinie Tatrzańskiej w listopadzie 2021 r. zarząd MiŚOT SA poinformował, że mali i średni operatorzy telekomunikacyjni staną się akcjonariuszami spółki, która stoi na czele grupy kapitałowej zbudowanej przez Stowarzyszenie e-Południe. W momencie rozpoczęcia prac nad nową strukturą 100-procentowym akcjonariuszem spółki akcyjnej było Stowarzyszenie e-Południe.

Przygotowano propozycje zmiany postanowień statutu spółki, sporządzono – zgodnie z obowiązującymi przepisami prawa – aktualizację wycen wartości podmiotów przeznaczonych do wniesienia do niej aportem. Pod koniec 2021 r. odbyło się Nadzwyczajne Walne Zgromadzenie MiŚOT SA. Zdecydowano na nim o niezbędnych zmianach treści statutu spółki, a także podwyższono jej kapitał zakładowy o wartość wniesionych aportem udziałów w spółkach: EPIX Sp. z o.o., Projekt MdO Sp. z o.o. i Projekt MdM Sp. z o.o. Wyrażono również zgodę na objęcie akcji przez członków Stowarzyszenia e-Południe. Komplet dokumentów niezwłocznie trafił do KRS. Po prawie pięciu miesiącach sąd zarejestrował zmiany.

– Rejestracja w KRS umożliwia formalne rozpoczęcie procesu udostępniania akcji dla MiŚOT-ów. Niestety, nie mieliśmy wpływu na tempo pracy KRS. Cieszymy się, że proces zakończył się pomyślnie – komentuje prezes MiŚOT SA Adam Kossowski.

Otwiera to drogę do dalszych kroków w udostępnianiu akcji operatorom, którzy są klientami spółek Grupy MiŚOT.

– Operatorzy, którzy staną się akcjonariuszami MiŚOT SA, nadal będą prowadzić własną działalność gospodarczą. Akcje spółki obejmą, jako osoby fizyczne, wspólnicy małych i średnich operatorów telekomunikacyjnych – przypominali członkowie zarządu MiŚOT SA podczas kwietniowego drugiego Lokalnego Zjazdu MiŚOT w Janowie Podlaskim. Uzasadniali też, że będzie to chronić spółkę przed utratą kontroli i wrogim przejęciem. Osoby fizyczne gwarantują większą stabilność w akcjonariacie spółki, podmioty gospodarcze podlegają częstym zmianom właścicielskim, są przedmiotem transakcji handlowych, generują ryzyko związane z prowadzoną działalnością gospodarczą, co mogłoby wpływać na bezpieczeństwo prawne i wizerunek spółki.

Wkrótce do operatorów zostaną wysłane listy intencyjne wraz ze wzorem deklaracji przystąpienia do spółki. Po ich podpisaniu możliwa będzie analiza poziomu zainteresowania nabyciem akcji przez operatorów, zostanie zbudowana tak zwana księga popytu. Otworzy to drogę do formalnego nabycia akcji przez MiŚOT-ów – poprzez zakup istniejących akcji od Stowarzyszenia e-Południe lub objęcie nowych walorów wyemitowanych w ramach podwyższenia kapitału zakładowego spółki.

– Mamy model udostępniania akcji. Będziemy premiować wieloletnią lojalną współpracę ze Stowarzyszeniem e-Południe i zakup naszych produktów. W tym celu stworzyliśmy bardzo przejrzysty algorytm. Dziś w EPIX-ie mamy ponad 850 uczestników i to oni na początku staną się właścicielami akcji MiŚOT SA – mówi Sebastian Kachel, wiceprezes Stowarzyszenia e-Południe i MiŚOT SA. ■

LoRaWAN BĘDZIE DZIAŁAĆ NA IPv6

MAREK NOWAK

Podczas codziennego korzystania z internetu dla użytkowników nie ma znaczenia, czy operatorzy używają protokołu IPv4 czy IPv6. Inaczej patrzą na to eksperci planujący rozwój projektów, które tworzone są na lata.

IP to skrót od angielskiej nazwy Internet Protocol. Dzięki temu protokołowi wszystkie sprzęty podłączone do internetu – komputer, laptop, smartfon, a także wszelkie inne urządzenia mieszczące się w pojęciu Internetu Rzeczy (ang. IoT czy Internet of Things) mogą wymieniać między sobą dane. Innymi słowy: to właśnie dzięki IP nasz laptop może komunikować się z urządzeniem osoby znajdującej się na drugim końcu świata.

Jak to działa?

Każde urządzenie ma też – co do zasady – swój indywidualny i niepowtarzalny adres (numer) IP. Od wielu lat do nadawania takich adresów używano IPv4, czyli czwartej wersji protokołu internetowego. Został on stworzony jeszcze w latach 80. ubiegłego wieku, a różne kombinacje cyfr w adresie pozwalają łącznie na utworzenie ok. 4,3 miliarda adresów. Ówcześnie wydawało się to ogromną i w pełni wystarczającą liczbą. Nie sądzono też, że internet stanie się tak popularny jak obecnie.

– Adresy protokołu IPv4 wyczerpały się już w 2019 roku – mówi Tomasz Brol, ekspert projektu MdI. – Po kilkudziesięciu latach od jego opracowania doszło do przełomu, którego nikt się nie spodziewał. Na świecie pojawiły się miliardy urządzeń podłączonych do sieci, a każdy taki sprzęt potrzebuje przecież unikalnego numeru, aby wymiana danych przebiegała bezproblemowo.

Co ciekawe, adres IP posiada także każda strona internetowa. Nie musimy go jednak pamiętać, ponieważ system DNS (Domain Name System) odpowiada za to, aby zamieniać trudne do zapamiętania numery IP na adresy zapisywane w dobrze znanej nam formie.

– Wyczerpanie się adresów IPv4 coraz częściej wymusza na operatorach stosowanie rozwiązań, w których jeden adres IP przypisany jest wielu użytkownikom, a on sam pośredniczy, oczywiście we w pełni zautomatyzowany sposób, za pomocą odpowiedniej bramki, w przekazywaniu treści do konkretnych urządzeń – wyjaśnia Tomasz Brol. – Adresy IPv4 są także odzyskiwane z niedziałających już stron czy urządzeń. Warto przy tym zauważyć, że istnieje też kolejka do nowego-starego adresu IPv4.

Coraz częściej słyszymy w związku z tym, że wcześniej czy później protokół IPv4 zostanie zastąpiony przez IPv6. Także RIPE Network Coordination Centre (niezależna organizacja wspierająca infrastrukturę sieci Internet) zachęca do tego, aby nowszy protokół był coraz częściej wybierany i rozwijany.

IoT wymaga IPv6

– W skali globalnej jesteśmy teraz w swoistym pacie – twierdzi Tomasz Brol. – Twórcy kontentu, urządzeń i operatorzy sieci patrzą na siebie nawzajem, a choć wszyscy wiedzą, że wcześniej czy później będą zmuszeni przestawić się na IPv6, nikt nie chce zrobić tego pierwszy. Wynika to z braku realnego zapotrzebowania rynku oraz konieczności poniesienia pewnych kosztów. Uznaliśmy jednak, że wprowadzając na rynek rozwiązania z zakresu Internetu Rzeczy, które mają działać przez lata, konieczne jest zrealizowanie ich na bazie nowego protokołu.

Nowe adresy IP składają się z ośmiu 16-bitowych części, oddzielonych od siebie dwukropkiem. Jest to 128-bitowa liczba, co daje możliwość stworzenia 340 sekstylionów adresów (nam także trudno zrozumieć wielkość tej liczby). Przykładowy adres IPv6 wygląda tak: 8098:a711:4240:5780:1f9b:1b93:1625:XXXX, przy czym zamiast każdego z iksów można wstawić dowolną cyfrę szesnastkową. IPv6 prawdopodobnie będzie więc w stanie wytrzymać wiele dekad i w końcu zapewne stanie się najpowszechniejszym rodzajem protokołu. Warto jednak dodać, że IPv6 po raz pierwszy pojawił się już w latach 90. ubiegłego wieku, gdy jeszcze nie sądzono, że pula adresów IPv4 może ulec wyczerpaniu, a rozwój technologiczny ponownie może nas zaskoczyć.

Jak już wspomnieliśmy, dla przeciętnego użytkownika różnica pomiędzy IPv4 a IPv6 jest niezauważalna. O wiele ważniejsze podczas codziennego korzystania z sieci jest szybkie, niezawodne łącze internetowe, które pozwoli bezproblemowo przesyłać i odbierać dane.

W przypadku rozwiązań z zakresu IoT posiadanie przez konkretne urządzenie własnego adresu IP ma znaczenie rosnące wraz z rozwojem tej technologii.

– Rozpoczynając w ramach Grupy MiŚOT budowę ogólnopolskiej sieci LoRaWAN, zdecydowaliśmy, że będzie ona działać na IPv6 – podsumowuje Tomasz Brol. – Dodatkowym plusem takiego rozwiązania jest możliwość przetestowania wprowadzenia nowego protokołu we względnie bezpiecznych warunkach. Pierwsze urządzenia zostały już pomyślnie zamontowane – dodaje. ■

Podsumowanie wybranych różnic między IPv4 i IPv6:

— Liczba bitów
- **IPv4:** długość 32 bitów, adres podzielony na cztery części 8-bitowe
- **IPv6:** długość 128 bitów, adres podzielony na osiem części 16-bitowych

— Sposób adresowania
- **IPv4:** numeryczny – poszczególne bity oddzielone kropkami. Same bity w zapisie dziesiętnym
- **IPv6:** alfanumeryczny – poszczególne bity oddzielone dwukropkami. Same bity w zapisie szesnastkowym

— Liczba dostępnych adresów
- **IPv4:** ok. 4,3 miliarda (wyczerpane)
- **IPv6:** ok. 340 sekstylionów

— Sposób przydzielania adresu do urządzenia
- **IPv4:** ręcznie (przez APIPA lub DHCP)
- **IPv6:** autokonfiguracja (urządzenie generuje adres, gdy połączy się z siecią dzięki IRDP i NDP)

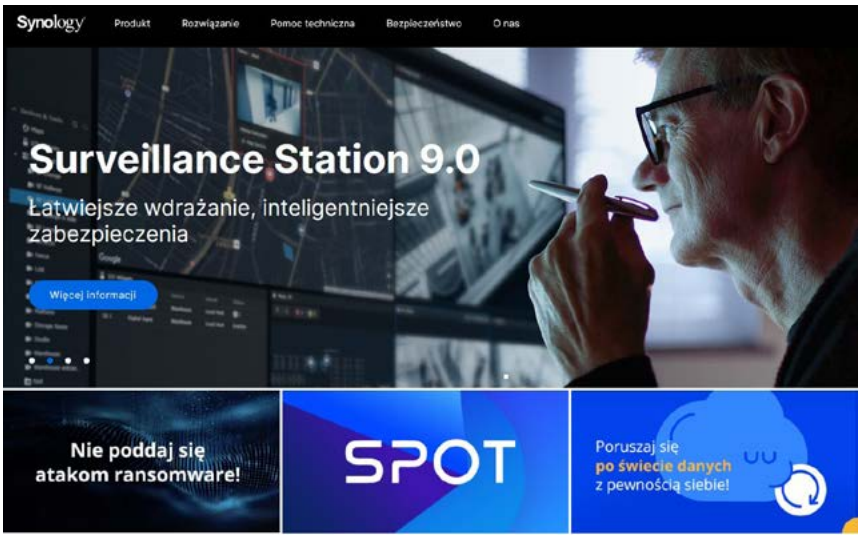
— Sposób konfiguracji
- **IPv4:** ręcznie albo przez DHCP
- **IPv6:** autokonfiguracja

— IPSec protokół zapewniający bezpieczeństwo i uwierzytelnianie danych
- **IPv4:** nieobowiązkowy, może być w pełni zintegrowany
- **IPv6:** obowiązkowy, w pełni zintegrowany

NOWOŚCI SKLEPU MiŚOT

KAROL BORYSOW

MiŚOT SA został partnerem marki Synology o statusie Gold Certified. Ma to praktyczne znaczenie dla oferty i funkcjonalności Sklepu MiŚOT.



– Nasi pracownicy, których Synology określa odtąd mianem inżynierów, pomyślnie przeszli szkolenia zakończone otrzymaniem imiennych certyfikatów – mówi Paweł Białas, dyrektor sprzedaży i rozwoju Grupy MiŚOT. – Jako Partner o statusie Gold Certified nie tylko otrzymujemy wsparcie techniczno-handlowe, ale również wypracowujemy system upustów, przez co możemy zaproponować niższe ceny zakupu wszystkich urządzeń naszego partnera MiŚOT-om. Dodatkowo wyszkolona kadra MiŚOT SA może wspierać operatorów przy realizacji wdrożeń u klientów biznesowych.

Inżynierowie MiŚOT SA posiadają obecnie certyfikaty DSM Architect oraz Backup Architect – zapowiadają jednak, że na tym jeszcze nie koniec.

– Już niebawem chcemy wzmocnić ofertę Synology dla MiŚOT w obszarze monitoringu i dlatego już wkrótce do naszego sklepu dołączą produkty Surveillance Device License Pack. Będziemy mogli także zaproponować wsparcie techniczno-handlowe dla Surveillance Station – dodaje Paweł Białas.

Dalsze decyzje dotyczące kierunków rozwoju i produktów sklepu MiŚOT podjęte będą po zakończeniu całego procesu szkoleń i certyfikacji Synology. Koordynatorzy nie wykluczają przy tym wprowadzenia do oferty innych rozwiązań, zależnie od potrzeb sygnalizowanych przez operatorów.

W Sklepie MiŚOT dostępne są obecnie także różne warianty usługi Publikon, szkolenia Akademii MiŚOT oraz (nieodpłatnie) dokumenty przygotowane w ramach akcji Internet od LOKALNI dla Uchodźców z Ukrainy.

Założona w 2000 r. firma Synology koncentruje się na zarządzaniu światowymi danymi i ich ochronie. Umożliwia przedsiębiorstwom zarządzanie danymi oraz ich zabezpieczenie bez względu na to, czy dostęp do nich jest uzyskiwany przez napęd flash, dysk lub architektury wielochmurowe. Firma dokonała już ponad sześciu milionów instalacji. ■

Sklep MiŚOT znajdziecie pod adresem sklep.misot.pl

sklep.misot.pl

MULTIMETRO TELEODPOWIEDZIALNYM ROKU 2021

PAWEŁ GNIADEK

TeleOdpowiedzialnym Roku 2021 została mikołowska firma Miconet posługująca się marką handlową Multimetro. Wśród wyróżnionych znalazły się: Interkonekt (Fiber), Fiberway i Pasjo.net (Piekary.net). Organizatorzy przyznali również dwa wyróżnienia specjalne za wsparcie pomocy Ukrainie. Otrzymały je Syrion i FajnyNet.

Rozstrzygnięcie kolejnej edycji konkursu TeleOdpowiedzialny Roku 2021 nastąpiło podczas uroczystej gali na Lokalnym Zjeździe MiŚOT w Janowie Podlaskim. 28 kwietnia nagrody na scenie wręczali: wiceprezes Stowarzyszenia e-Południe Sebastian Kachel, prezes Fundacji Lokalni Daniel Piecuch oraz przedstawiciel sponsora konkursu – Rafał Jach, dyrektor Działu Sprzedaży w XBEST.PL.

– Z roku na rok rośnie zainteresowanie naszą inicjatywą i poziom przesyłanych do oceny aplikacji. To był wyjątkowy konkurs. Otrzymaliśmy trzy razy więcej zgłoszeń niż w poprzednim roku. Jest to najlepszym świadectwem, że mali i średni operatorzy telekomunikacyjni byli i są społecznie odpowiedzialni – powiedział Sebastian Kachel.

W tym roku szczególne uznanie członków kapituły, składającej się z ekspertów branżowych, naukowców i przedstawicieli mediów, zyskały działania CSR prowadzone w 2021 roku przez Multimetro. Nagrodę w imieniu firmy odebrali Grzegorz Długaj i Klaudia Skutela, podkreślając, że zwycięstwo w konkursie zmobilizuje firmę do jeszcze większej aktywności w obszarze społecznej odpowiedzialności biznesu.

Michał Żukrowski z niepołomickiej firmy Fiberway oraz Grzegorz Czempik i Sebastian Haider, wspólnicy firmy Pasjo.net z Piekar Śląskich, która posługuje się marką handlową Piekary.net, również dziękowali za wyróżnienia.

Na gali odczytano też list od Pawła Barczyka i Tomasza Furmana, reprezentujących trzeciego wyróżnionego konkursowicza – firmę Interkonekt z Wolbromia, która jest operatorem sieci światłowodowej Fiber.

Wszystkie aplikacje zgłoszone w konkursie zasilą Bazę Dobrych Praktyk tworzoną przez Grupę MiŚOT. Operatorzy będą mogli z niej czerpać, planując aktywność CSR na swoim terenie.

– Warto dzielić się z MiŚOT-ami swoimi projektami, będziemy je promować i wspierać operatorów. Mam nadzieję, że nasza baza stanie się też inspiracją dla wielu operatorów – poinformował prezes Fundacji Lokalni Daniel Piecuch.

W tej edycji podmioty najaktywniejsze w obszarze CSR otrzymały atrakcyjne nagrody ufundowane przez organizatorów oraz sponsora konkursu – firmę XBEST.PL.

Konkurs TeleOdpowiedzialny Roku cieszy się coraz większą popularnością, z roku na rok zwiększa się liczba zgłoszeń. W ubiegłym roku laureatem została poznańska Systemia.pl, zaś w 2019 roku – Interkonekt. ■

Filmy prezentujące zwycięzcę konkursu TeleOdpowiedzialny Roku 2021 oraz wyróżnionych:

Miconet Fiberway Interkonekt Piekary.net Syrion

AKTYWIZACJA SPOŁECZNO-ZAWODOWA OSÓB Z NIEPEŁNOSPRAWNOŚCIAMI W TELECENTRUM

MAREK NOWAK

Już cztery fundacje aktywizujące osoby niepełnosprawne współpracują z TeleCentrum, które wspiera małych i średnich operatorów telekomunikacyjnych z całej Polski, odciążając pracę biur obsługi klienta. Jedną z tych organizacji jest Fundacja Aktywnej Rehabilitacji.

FAR od lat aktywizuje osoby niepełnosprawne. Początki działalności fundacji sięgają 1988 roku, kiedy to odbył się pierwszy w Polsce obóz wprowadzający. Dwunastu szwedzkich instruktorów, realizując cel propagowania aktywnej rehabilitacji, przekazało Polakom swoje metody i pomogło we wprowadzaniu ich w życie. Od tego czasu idea, że powrót do społeczeństwa jest kwestią woli osoby niepełnosprawnej i że ludziom z uszkodzonym rdzeniem kręgowym trzeba stworzyć warunki do samodzielnego decydowania o sobie, realizowana jest w praktyce.

Fundacja i TeleCentrum współpracują w ramach realizowanego obecnie Regionalnego Programu Operacyjnego pod nazwą „Aktywizacja społeczno-zawodowa 40 osób z niepełnosprawnościami z województwa śląskiego szansą na aktywność i niezależność". Jest on dofinansowany ze środków unijnych.

– Oddział śląski FAR w Mikołowie prowadzi zarówno projekty wieloletnie obejmujące szeroko pojęte przystosowanie społeczne osób po wypadkach, w tym na przykład technikę jazdy na wózku, jak i krótsze (nawet weekendowe), ukierunkowane na ich aktywizację społeczno-zawodową – mówi Katarzyna Lipka, trenerka pracy FAR. – Można powiedzieć, że specjalizujemy się w projektach wspierających osoby na wózkach, co związane jest z tym, że w skład naszej kadry wchodzą osoby, dla których jest to także codziennym doświadczeniem. W poszczególnych prowadzonych przez nas projektach uczestniczą jednak również amazonki, osoby niedowidzące i głuchonieme.

Niełatwa praca

Zatrudnienia w TeleCentrum od początku mają dodatkowy akcent społeczny. Ponad 75 proc. jego pracowników to osoby niepełnosprawne. W zespole pracują obecnie osoby w wieku od 26 do 60 lat. Część z nich znalazło pracę w TeleCentrum właśnie za pośrednictwem Fundacji Aktywnej Rehabilitacji oraz Fundacji Aktywizacja. Kolejnymi organizacjami, które współpracują z TeleCentrum, są Ratownik Górniczy Fundacja Pomocy Osobom Niepełnosprawnym i Stowarzyszenie SPOZA, które także pragnie pomagać osobom niepełnosprawnym w pokonywaniu barier psychicznych i społecznych związanych z niepełnosprawnością.

– Realizowany obecnie projekt nie jest też pierwszym, który realizujemy wspólnie w Fundacją Aktywnej Rehabilitacji – stwierdza Marcin Pilak, koordynator projektu TeleCentrum. – Z czasem lepiej się poznaliśmy, pracownicy fundacji zrozumieli specyfikę naszej pracy, a teraz prowadzą już nawet preselekcję kandydatek i kandydatów. Bardzo cenię osoby niepełnosprawne, które chcą pracować, ale też na własnej skórze przekonałem się, że praca w TeleCentrum nie jest łatwa. Wymagana jest przede wszystkim duża odporność na stres, ponieważ zdarzają się sfrustrowani klienci, a nawet tacy, którzy obrażają naszych agentów. Oczywiście należy w takich przypadkach przerwać rozmowę, ale trzeba też radzić sobie z nieprzyjemnymi emocjami.

Oprócz odbierania połączeń od klientów lokalnych operatorów z całego kraju, agenci przeprowadzają także zlecone akcje marketingowe, sondaże i badania satysfakcji klienta.

– Osobiście poznałam specyfikę pracy w telefonicznym biurze obsługi klienta i zdaję sobie sprawę, że nie każdy się w niej odnajdzie – zaznacza Katarzyna Lipka. – W ramach szczerej rozmowy z beneficjentami naszego programu przekazuję im plusy i minusy, przedstawiam fakty (głównie obowiązki i wymagania), opowiadam też o swoich doświadczeniach i mówię wprost, że osoby nieśmiałe nie dadzą rady.

Ostateczną decyzję o stażu podejmują jednak sami beneficjenci.

Rekrutacja i rozwój

TeleCentrum rozwija się. Zapotrzebowanie na wspólne call center MiŚOT, które działa w trybie całodobowym przez wszystkie dni tygodnia, nadal jest duże. Aktualnie korzysta z tego około 60 firm, prowadzone są też nowe wdrożenia. Na ten rok planowane jest także zwiększenie zakresu usług świadczonych przez agentów.

– Od dłuższego czasu jesteśmy właściwie w trakcie nieustannej rekrutacji. Z jednej strony zwiększamy zatrudnienie, a z drugiej mamy po prostu dynamiczną sytuację w zespole – przyznaje Marcin Pilak. – Część osób, które dzięki TeleCentrum nabyły nowych kompetencji, doświadczenia i śmiałości w kontaktach międzyludzkich, po prostu postanawia ruszyć dalej – dodaje. ■

Kontakt ze śląskim biurem Fundacji Aktywnej Rehabilitacji:
tel. kom.: 508 015 916
e-mail: biuro.slaskie@far.org.pl

Adres kontaktowy w sprawie pracy w TeleCentrum: cc@telecentrum.misot.pl

TeleCentrum rozwija się. Zapotrzebowanie na wspólne call center MiŚOT, które działa w trybie całodobowym przez wszystkie dni tygodnia, nadal jest duże.

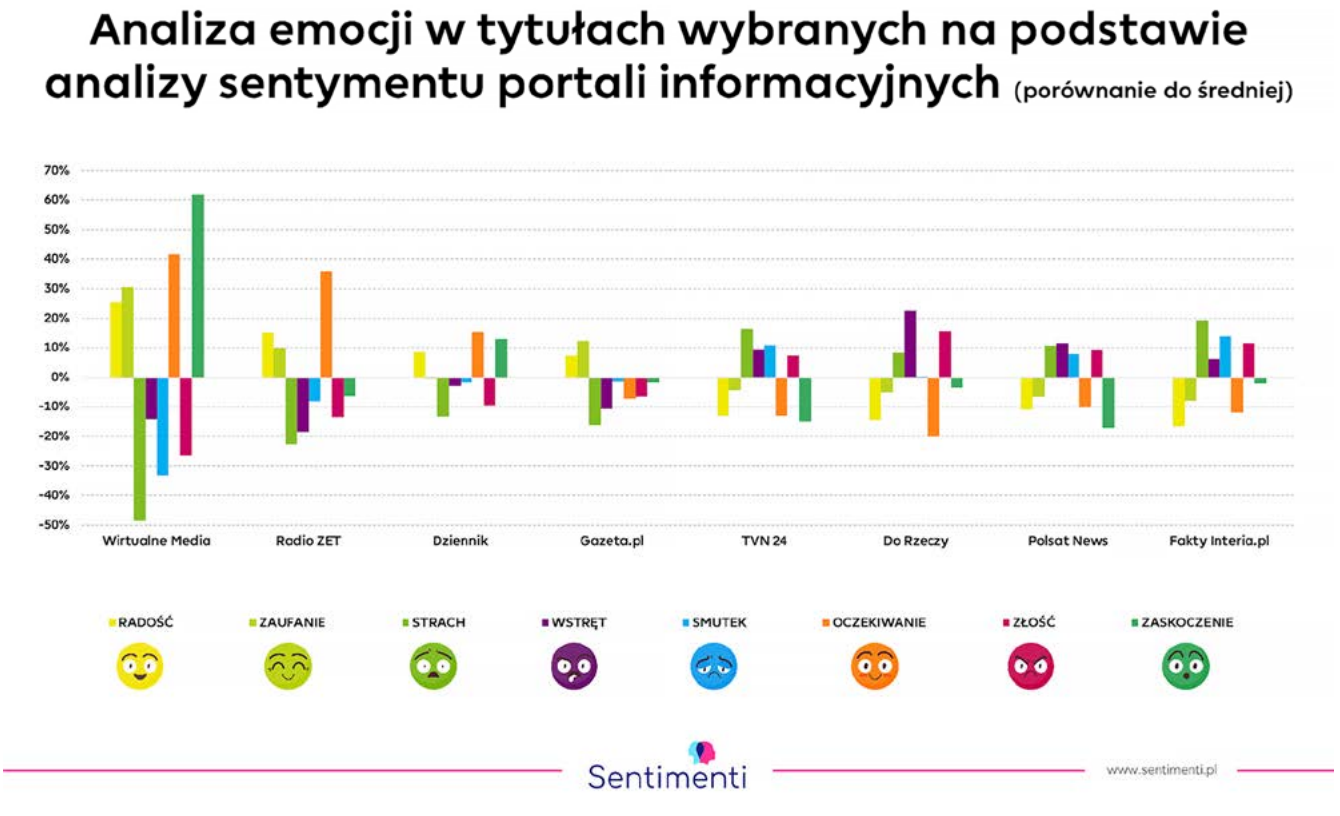
TWÓJ OPERATOR DOBRA

MARCIN OROCZ

Projekt Lokalni.pl zmienia się. Po wysłuchaniu wielu opinii i uwag, przeanalizowaniu, co działało, a co nie, wybraliśmy kilka pomysłów, które udało się zrealizować i które są obecnie w fazie testów. By dołączyć do testerów nowej odsłony Lokalnych, zapraszam na ISPForum.pl.

W nowej odsłonie prezentujemy rozbudowany zestaw narzędzi marketingowych i promocyjnych zwiększających zasięgi i generujących leady, a nawet przynoszących na „tacy" klienta. I tu mógłbym dużo pisać o tym, jak wykorzystujemy SEO*, SEM** i Growth Hacking***, które stosujemy, by za pośrednictwem marki Lokalni.pl przyciągnąć ruch i rozdysponować go pośród MiŚOT-ów zgłoszonych do programu. Będzie się sporo działo w warstwie cyfrowej i komunikacji online, lecz nie tylko w mediach społecznościowych, kanałach wideo czy na samym portalu. Chciałbym, żeby najpierw zadziało się w sercach.

Nowoczesny marketing oparty jest na emocjach i wartościach, które inspirują ludzi do podejmowania konkretnych działań i osiągania najlepszych efektów. Możemy badać, jakie emocje towarzyszą ludziom czytającym dany artykuł, i odpowiednio dobierać treści, by skuteczniej budować swój wizerunek.



(źródło sentimenti.pl)

Lokalni.pl mają budzić zaufanie, dawać ludziom radość, pobudzać oczekiwania i pozytywnie zaskakiwać. Dlatego na portalu będziemy nagłaśniać wasze inicjatywy, pokazywać, jak pomagacie lokalnej społeczności oraz jak poprzez wasze zaangażowanie i drobne gesty podnosi się jakość życia lokalnej społeczności. Pisząc wprost, chcę, by dobro, które od lokalnych operatorów wychodzi, do lokalnych społeczności wracało. Aby twój odruch serca chwytał za serce i budował wizerunek twojej marki jako tej, której warto zaufać i z którą warto się związać na lata.

ChceMiSie

Dzielenie się dobrem to nie taka prosta sprawa, a chwalenie się tym wywołuje refleksje typu „a po co?", „niech nie wie lewa ręka, co czyni prawa", „nie robię tego na pokaz". Słusznie, bo tu nie o uczynki chodzi, a motywację. Nie robimy tego na pokaz i nie z tego powodu pomagamy innym. To jest nasz odruch serca. I warto, żeby był doceniony, żeby o nim napisać, żeby skupić na chwilę na nim uwagę i dać przykład innym do działania. Najtrudniej jest być samotnym w działaniu, więc jeżeli pokażemy, że w czynieniu dobra dla innych jest nas więcej, będzie się nam bardziej chciało, będziemy w tym bardziej konsekwentni, a wykorzystując potencjał grupy, jaką stanowimy, możemy osiągnąć skalę, która nie tylko będzie przemieniać nasze małe społeczności, ale też wyjdzie poza granice (co już nam się nieraz udało).

Co robimy?

Zgłoś nam swoją inicjatywę, a my wykorzystamy najnowsze możliwości technologii, by profesjonalnie o tym opowiedzieć. Spraw, by Twoje dobro inspirowało innych. Jak to zrobić?

Wejdź na lokalni.pl i wypełnij formularz „dodaj dobro". Skontaktujemy się z tobą i omówimy szczegóły. Po zaakceptowaniu materiałów nagłośnimy twoje dobro nie tylko na portalu lokalni.pl, ale także w zaprzyjaźnionych mediach lokalnych i sieciach społecznościowych. Tak, by wzmocnić twój wizerunek Dobrego Operatora wspierającego lokalne społeczności. Stworzone w ten sposób historie umieścimy na mapie dobra, tak aby każdy mógł znaleźć w swojej okolicy MiŚOT-a z dobrym serduchem, gotowym do pomagania. ■

Wejdź na lokalni.pl i wypełnij formularz „dodaj dobro". Skontaktujemy się z tobą i omówimy szczegóły. [...] Stworzone w ten sposób historie umieścimy na mapie dobra, tak aby każdy mógł znaleźć w swojej okolicy MiŚOT-a z dobrym serduchem, gotowym do pomagania.

WAŻNE POJĘCIA

SEO (Search Engine Optimization) – proces, którego celem jest osiągnięcie przez stronę internetową jak najlepszej pozycji w bezpłatnych (naturalnych, organicznych) wynikach wyszukiwania dla wybranych fraz i słów kluczowych.

SEM (Search Engine Marketing) – marketing w wyszukiwarkach, czyli ogół działań promocyjnych, które mają podnieść pozycję danego serwisu w wynikach wyszukiwania (zarówno naturalnych, jak i płatnych) przy użyciu odpowiednio dobranych fraz lub słów kluczowych, wpisywanych przez użytkowników podczas poszukiwania informacji w wyszukiwarkach.

Growth Hacking (hakowanie wzrostu) – działania skupione wokół pełnego lejka sprzedażowego/marketingowego, oparte o dane i szybkie testowanie kolejnych hipotez, w celu zbudowania wzrostu, najczęściej w przedsiębiorstwach, które nie mają dużego budżetu na marketing, ale zachowują szansę na duży i szybki wzrost.

MILIONY DLA LOKALNYCH OPERATORÓW

MICHAŁ KOCH

Projekt MdO, czyli MiŚOT dla Ogólnopolskich, umożliwił MiŚOT-om start pod wspólną marką w przetargach na budowę Ogólnopolskiej Sieci Edukacyjnej. Dzięki temu zrównano szanse w stosunku do operatorów korporacyjnych, a mniejsi operatorzy odnieśli sukces – pozyskali w latach 2018–2021 w postępowaniach organizowanych przez NASK ponad 3000 lokalizacji.

W MdO uczestniczy kilkuset MiŚOT-ów. Dzięki udziałowi w przedsięwzięciu otrzymali oni w 2021 roku prawie 10 mln zł, a szacowane przychody do 2025 roku przekroczą 45 mln zł.

Wyniki MdO to przede wszystkim efekt założeń projektowych, które uwzględniły zdolność lokalnych operatorów do partycypacji w przetargach NASK. Dzięki dobrej koordynacji pracy i zaangażowaniu kierowników projektu oraz pracowników Grupy MiŚOT udało się przygotować sprawny system zgłaszania udziału, wykonywania usługi i konserwacji OSE.

Klaudia Markwat, dyrektor ds. współpracy z operatorami NASK, o projekcie wypowiada się następująco: – Od września 2018 r. do lutego 2022 r. odebraliśmy od MDO i uruchomiliśmy usługę OSE dla ponad 3 000 łączy do szkół. Na początku projektu mieliśmy problemy komunikacyjne, ale w tej chwili wypracowaliśmy standardy współpracy i podłączanie szkół przebiega bardzo sprawnie. Jako przedstawiciele administracji publicznej musimy działać w oparciu o procedury, jednak wydaje się, że uprościliśmy je na tyle, że są one zrozumiałe.

– Istotne z punktu widzenia NASK jest to, że dzięki MDO docieramy do lokalnych operatorów i możemy obsłużyć szkoły, które znajdują się poza kręgiem zainteresowania dużych firm telekomunikacyjnych, na terenach gorzej zurbanizowanych. Z kolei sukcesem MDO jest niewątpliwie efektywne konkurowanie z innymi operatorami i zdobycie kontraktów na pięć lat – dodaje Klaudia Markwat.

Spółka nadal uczestniczy w postępowaniach na budowę OSE i jednocześnie przygotowuje się do kolejnych przetargów o szerokim zasięgu, w których wykorzysta potencjał MiŚOT-ów oraz własne doświadczenie.

MdO to jedna z najważniejszych inicjatyw Grupy MiŚOT. Ostatnie miesiące przyniosły również rozwój strukturalny. W przyszłości MdO zmieni się w rozwiązanie komercyjne dla wszystkich lokalnych operatorów, którzy planują rozwój infrastruktury i dotarcie do nowych klientów. Dzięki zdobytemu know-how możliwy będzie start w innych ogólnopolskich przetargach związanych ze świadczeniem usług dostępu do sieci.

Lokalni operatorzy pokazali, że mogą stawać do ogólnopolskich postępowań i zdobywać lokalizacje, które na pierwszy rzut oka wydają się trudne do podłączenia. To właśnie świadczy o ich sile i zaradności. Zainteresowanie udziałem w przetargach przekuto w realne działanie. ■


ISPORTAL
publikon
KODEKS SPOŁECZNEJ ODPOWIEDZIALNOŚCI BIZNESU BRANŻY TELEKOMUNIKACYJNEJ
Branżowy kodeks CSR w nowej odsłonie
Zdalnie byłoby trudniej
Pierwszy z cyklu Zjazdów MiSOT wyprzedany
Nie bagatelizujmy inflacji
Jak usprawnić marketing firmy?
Ludzie Grupy MiSOT... czyli ci, którzy pracują dla Was: Marcin Orocz...
Mali płacą więcej
Pierwsza partia procesorów Bajkał II generacji opuściła tajwańskie zakłady TSMC
Ludzie Grupy MiSOT... czyli ci, którzy pracują dla Was: Marcin Orocz.
WWW.ISPORTAL.PL

PUBLIKON UZUPEŁNIA INNE FORMY PROMOCJI

KAROL BORYSOW

Publikon buduje wizerunek firmy i pomaga małym i średnim operatorom telekomunikacyjnym w sprzedaży usług. Korzystanie z niego nie zastępuje jednak innych form promocji. O tym, jak je sprawnie połączyć, rozmawiamy z Sebastianem Pycią.

Jakie masz doświadczenie we współpracy z Publikonem?

Sebastian Pycia: Jako Art-Com byliśmy jednym z jego pierwszych klientów. Jestem też osobiście zaangażowany w projekt Lokalni, więc nie było się nad czym zastanawiać.

Korzystacie w związku z tym z najdroższego pakietu?

SP: Nie, ze średniego. Publikon nie jest jednak naszą jedyną ani główną aktywnością w mediach społecznościowych, traktuję go raczej jako wsparcie. Sam także jestem bardzo aktywny i praktycznie codziennie – nawet w weekendy – wykorzystuję największą siłę tej formy kontaktu, czyli interaktywność. Kiedy klienci piszą – odpowiadam.

Publikon promuje lokalność, przekazuje też praktyczne informacje. Jeden z postów przypominał, że pakiety usług są bardziej opłacalne i można je znaleźć u lokalnych dostawców w połączeniach skrojonych do potrzeb odbiorców. Jakie posty wrzucasz osobiście?

SP: Konkrety z lokalnego rynku. Na przykład o tym, że wchodzimy na nową dzielnicę, organizujemy promocję, konkurs, wspieramy jakiś event lub festyn. Jesteśmy na każdej większej imprezie organizowanej przez miasto, takiej jak choćby obchody Dnia Dziecka. Rozdajemy tam gadżety, zapewniamy też atrakcje, takie jak fotobudka, która cieszyła się bardzo dużą popularnością.

Jakie macie jeszcze sposoby promocji i szukania klientów?

SP: Przyczepka, banery, a także gadżety, takie jak torby bawełniane, kalendarze z naszym logo i zdjęciami Jaworzna, smycze, długopisy. Czasem nawet rozsyłamy je losowo i przynosi to zaskakująco dobre efekty. Dziś z pewnością mogę powiedzieć, że jesteśmy dobrze rozpoznawalni lokalnie.

Jak to osiągnęliście?

SP: Na budowanie marki składa się wiele małych rzeczy, musi też odbywać się to konsekwentnie i trwać dłuższy czas.

Z czego moglibyście dziś zrezygnować w promocji usług?

SP: Jeśli mam jakieś wątpliwości, to dotyczą one papierowych ulotek. To trochę przeżytek, a do tego są mało ekologiczne. Z pewnością nie zrezygnowałbym z Publikona. Cena w stosunku do korzyści w postaci zewnętrznego wsparcia grafika i przygotowania profesjonalnych treści jest tu bardzo dobra. ■


NAJLEPSZA USŁUGA PUBLIKACJI POSTÓW
NA TWOIM PROFILU FIRMOWYM W BRANŻY ISP
JUŻ OD 99 ZŁ / M-C
ZAMÓW I ZARABIAJ WIĘCEJ JUŻ DZIŚ!
publikon
PUBLIKUJEMY U CIEBIE
Lokalne usługi
to wsparcie swojego regionu!
Rewelacyjne ceny
lokalne wsparcie

GRILL Z ISP FORUM 5

Grillowanie trwa!

MICHAŁ KOCH

Grill must go on! Piąta część przeglądu najciekawszych wątków z ISP Forum.

Na ISP Forum trwają rozmowy dotyczące agresji Rosji na Ukrainę i cyberbezpieczeństwa w czasie wojny. „Historia dzieje się na naszych oczach" – to zdanie otwierające dyskusję o obecnej sytuacji międzynarodowej. Dwa wspomniane tematy to „Ukraina–Rosja – czy możemy pomóc?" oraz „Obowiązujące stopnie CRP i ich konsekwencje dla MiŚOT – MdS radzi".

Świat obiegły informacje o trwających atakach sieciowych. Hakerzy walczą po obu stronach, a problemy z dostępem do różnych witryn internetowych odnotowano też w Polsce. Marcin Zemła, przedstawiciel projektu MdS (MiŚOT dla Security), apelował o spokój i metodyczne, chłodne działanie. Ekspert odniósł się też do wprowadzonego alarmu CHARLIE-CRP: „[stan alarmowy – przyp. MK] wiąże się dla niektórych z Was z pewnymi obowiązkami ustawowymi. Podmioty obsługujące administrację publiczną mają pomóc w ich wykonaniu. Zatem jeśli, moi drodzy, wśród Waszych klientów znajdują się jednostki publiczne […] mają wesprzeć w zakresach wynikających z umów jednostki administracji publicznej".

Eksperci przedstawiają skalę zjawiska. Polskie serwery mierzą się z milionami ataków typu C2C, próbami wszczepienia złośliwego kodu oraz łamania zaszyfrowanych danych. „Wojna w cyberprzestrzeni trwa" – podsumował Zemła. Operatorzy informują, że obserwują coraz więcej podejrzanych aktywności w logach własnych sieci.

Operatorzy zwrócili też uwagę na problem fake newsów. Na ich temat Marcin Zemła wypowiedział się następująco: „Dezinformacja jest jednym z elementów wojny hybrydowej". Operatorzy na ISP Forum dyskutowali również o działaniach grupy hakerów Anonymous.

W Jędrzychowie nie chcą słupów

O słupach światłowodowych w Jędrzychowie pisaliśmy na ISPortal.pl. Mieszkańcy nie chcą drewnianych słupów. Ich zdaniem kable powinny zostać poprowadzone w ziemi. Sprawę skomentowali operatorzy telekomunikacyjni na ISP Forum.

Mieszkańcy Jędrzychowa mają zastrzeżenia do realizacji projektu „Zielonogórski Orange Światłowód". Sieć powstaje na terenie Zielonej Góry, ale w Jędrzychowie uznano, że jest nieodpowiednio przeprowadzana.

Zdaniem Jędrzychowian miejsce światłowodów jest w instalacji podziemnej. Jeden z mieszkańców, obecny na forum przedstawiciel środowiska ISP, przyznał, że słupy stawia Orange, Enea i jeden z lokalnych operatorów, przez co mieszkańcy mają „kable za oknami".

Jeden z użytkowników forum obwinił ogólną politykę i antagonizmy przedsiębiorców. Jego zdaniem „wszystko to mogłoby z powodzeniem wisieć na jednym komplecie".

Czy jest alternatywa dla słupów? Cóż, pewnie mieszkańcy miasta mogliby wybudować odpowiednią kanalizację pod infrastrukturę. Lub korzystać z internetu radiowego. Czy to jednak odpowiednie rozwiązania? Forumowicze zgodnie stwierdzili, że koszty budowy w ziemi ostatecznie sprawiłyby, że wzrósłby abonament. I byłaby to kolejna bulwersująca sprawa dla mieszkańców. „Ja mam wszystko w ziemi, a tam, gdzie nie można dojść (głównie w sensie „nie opłaca się"), to nie wchodzę – no, chyba że klienci sami zapłacą" – napisał forumowicz.

„[…] teraz zmieśćmy to pod ziemią. Brak projektu/organizacji jest tu problemem" – padła inna odpowiedź, być może kluczowa do zrozumienia problemu.

Do dyskusji można dołączyć na ISP Forum.

DrMiŚOT

Popularnym miejscem wymiany poglądów jest też grupa na Facebooku znana jako drMiŚOT. Jest to prywatna grupa, która zrzesza wyłącznie przedstawicieli małych i średnich operatorów telekomunikacyjnych.

Grupa służy wymianie doświadczeń i dzieleniu się dobrymi praktykami – między nami MiŚOT-ami, a nad wszystkim czuwa niepokonany #drMiŚOT. ■

Przenoszenie ISP Forum

Switch PoE

Platforma transkodująca oraz odbiór DVB-T2

Łatajcie QNAPy

Szukam listwy RACK z przełącznikiem faz

Podwyżki abonamentu dla przyszłych i obecnych klientów

Internet dla uchodźców – umowa po ukraińsku i polsku

ALFA-CRP

Zmasowany atak na kamery Hikvision

Czy Rosja da radę wyłączyć internet na Ukrainie

Ukraina-Rosja - CYBER - czy możemy pomoc?

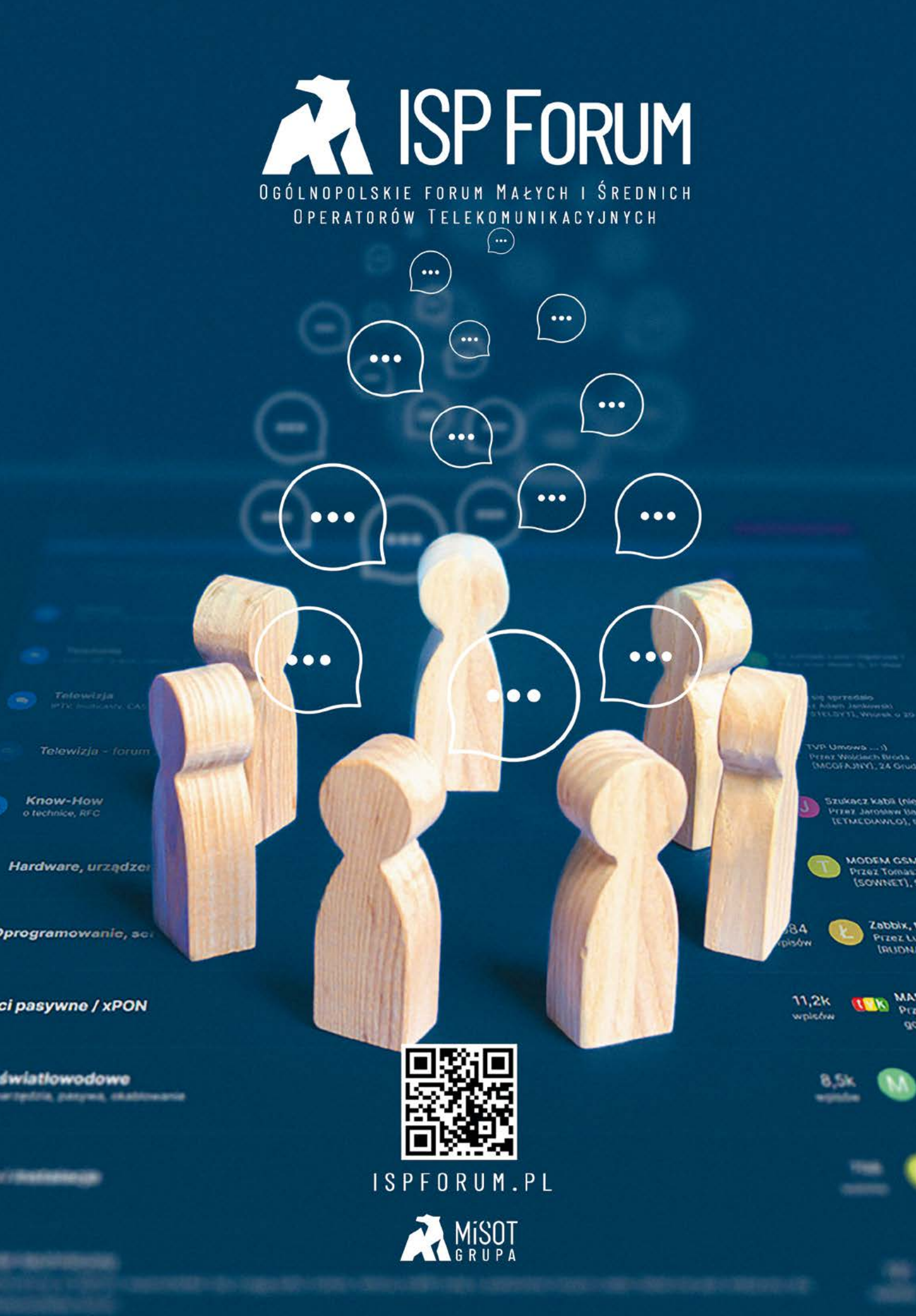
Obowiązujące stopnie CRP i ich konsekwencje dla MiŚOT - MdS radzi

Evio się sprzedało

Największy operator w Polsce przejęty

Remont klatki schodowej a dostęp do urządzeń

Audyt dot. gier hazardowych


ISP FORUM
OGÓLNOPOLSKIE FORUM MAŁYCH I ŚREDNICH
OPERATORÓW TELEKOMUNIKACYJNYCH
ISPFORUM.PL
MiSOT
GRUPA

Zjazd na zamku zobowiązuje - część artystyczna

MALI I ŚREDNI OPERATORZY ZJEDNOCZENI

Relacja z Lokalnego Zjazdu MiŚOT w Janowie Podlaskim

MICHAŁ KOCH, MAREK NOWAK, PAWEŁ GNIADEK

Zakończył się Lokalny Zjazd MiŚOT w Janowie Podlaskim. Wśród najmocniejszych punktów wydarzenia wymienić należy operatorski hyde park, bloki dotyczące cyberbezpieczeństwa oraz budowy polskiej sieci LoRaWAN.

Lokalny Zjazd MiŚOT w Janowie Podlaskim odbył się 28–29 kwietnia 2022 roku. Już jednak dzień wcześniej, w formule hyde parku, mali i średni operatorzy omówili najważniejsze, nurtujące ich sprawy. Z kuluarowych rozmów podczas całego zjazdu wynikało, że jednym z tematów była wówczas konieczność silniejszego wsparcia organizacji i inicjatyw broniących interesów małych i średnich operatorów telekomunikacyjnych, którzy konfrontują się obecnie z aktualną, niełatwą sytuacją na rynku.

O prawie, podatkach i inflacji

Pierwszego dnia konferencji eksperci i przedstawiciele MiŚOT poruszyli tematykę rosnącej inflacji oraz podnoszenia cen przez lokalnych operatorów. Ewelina Grabiec i Łukasz Bazański, przedstawiciele kancelarii prawnej itBlegal, próbowali znaleźć odpowiedź na pytanie, w jaki sposób operatorzy telekomunikacyjni mogą podnieść ceny za usługi, omawiając przy tym stanowisko Urzędu Ochrony Konkurencji i Konsumentów. Panel, w którym wziął udział także Konrad Baranowski, właściciel średniej wielkości przedsiębiorstwa telekomunikacyjnego ze ściany wschodniej, zdiagnozował aktualną sytuację, wskazując wśród istotnych problemów między innymi opieszałość w tworzeniu rozwiązań prawnych. – Weźmy pod uwagę na przykład kanalizację wewnątrzbudynkową – wskazywał Konrad Baranowski. – Przepisy są obecnie dobre, ale tworzone były bardzo długo.

Uczestniczący w dyskusji Tomasz Opolski z KPRM zapowiedział, że kwestia podniesienia cen zostanie uregulowana w sposób korzystniejszy dla operatorów w opracowywanej ustawie Prawo komunikacji elektronicznej. – Departament cyfryzacji zmierza już do ukończenia prac nad PKE – stwierdził, co jednak nie jest już pierwszą tego typu deklaracją. Panel obfitował również w omówienie niuansów prawnych, które obecne są w polskiej legislacji telekomunikacyjnej.

Polski Ład był natomiast przedmiotem bloku prowadzonego przez kancelarię Brightspot. Radcy prawni Katarzyna Orzeł i Maciej Jojczyk przede wszystkim wzięli pod lupę nowelizację przepisów, analizując, kto dzięki niej zyska, a kto straci.

O równą stawkę

Kolejnym ważnym momentem podczas pierwszego dnia zjazdu była prelekcja dotycząca tego, jakie skutki dla współpracy MiŚOT-ów z operatorami systemów dystrybucyjnych w zakresie wykorzystania słupów niesie decyzja sądu w spra-

Wystawcy z uśmiechem przywitali przybyłych gości


Prelekcje bogate w merytorykę


Spotkań czas!

Krzysztof Czuszek, Tomasz Brol, Artur Tomaszczyk

wie wstrzymania wykonalności decyzji ramowej Prezesa UKE dla Taurona.

– Sąd Ochrony Konkurencji i Konsumentów nie uzasadnił postanowienia wstrzymującego z grudnia 2021 roku – podkreśliła Ewelina Grabiec, która wyjaśniła ponadto, czego mogą spodziewać się przedsiębiorcy, którzy chcą w aktualnej sytuacji uzyskać dostęp do słupów Taurona. – W obowiązujących cennikach znajdziemy więc stawki podobne do tych sprzed decyzji ramowych – podkreśliła.

Ewelina Grabiec i prezes Krajowej Izby Komunikacji Ethernetowej Karol Skupień poprowadzili też kolejny panel. Dotyczył on opłat za zajęcie pasa drogowego.

– Mamy dziś do czynienia ze skrajnie niesprawiedliwą i dyskryminującą sytuacją – podkreślił Karol Skupień. – Operatorzy telekomunikacyjni należący do sektora małych i średnich przedsiębiorstw, którzy budowali sieci w pasie drogowym w latach 2003–2019, nadal objęci są obowiązkiem uiszczania opłat sięgających do 200 złotych za metr kwadratowy. Operatorzy rozbudowujący sieci po wejściu w życie nowelizacji płacą zdecydowanie mniej (do 20 złotych), a największy działający w Polsce operator telekomunikacyjny nie ponosi żadnych opłat za większość sieci umieszczonych w pasie drogowym. Usłyszeliśmy też, że KIKE dąży do zmiany tej sytuacji.

Przeciw publicznym operatorom

W dalszej części bloku KIKE Kinga Pawłowska-Nojszewska rozmawiała z przedstawicielami MiŚOT o Centrum Reputacyjnym Komunikacji Elektronicznej oraz rządowych koncepcjach nowych publicznych operatorów telekomunikacyjnych. Operatorzy krytycznie odnieśli się szczególnie do tej ostatniej koncepcji, która tworzy możliwość (a czasami wręcz obowiązek) przejmowania szerokiej gamy klientów przez publicznych przedsiębiorców.

Głos w dyskusji w sprawie projektu ustawy o zmianie ustawy o Służbie Więziennej oraz niektórych innych ustaw (USW) zabrał Maciej Syguła z firmy Ahmes (członek KIKE). Wskazał on, że projekt zakładający, że minister sprawiedliwości w drodze decyzji będzie wskazywał przywięziony zakład pracy (PZP), który świadczyć będzie usługi telefoniczne tymczasowo aresztowanym (obowiązkowo) oraz skazanym (fakultatywnie), w praktyce uniemożliwia mu prowadzenie działalności, w jakiej się wyspecjalizował.

Dowiedzieliśmy się też, że projekt omawianej ustawy nie wskazuje przy tym, iż każdy areszt śledczy i każdy zakład karny będzie obsługiwany przez odrębny PZP. Istnieje więc możliwość, że jeden taki zakład będzie obsługiwał nawet wszystkie te placówki. Status PZP może przysługiwać m.in. spółce, w której Skarb Państwa posiada więcej niż połowę udziałów lub akcji i której osoby pozbawione wolności stanowią co najmniej 20 proc. ogółu zatrudnionych, przy czym nie muszą to być osoby zatrudnione w pełnym wymiarze czasu pracy. Taką firmą mógłby stać się Exatel, którego przedstawiciel – Maciej Szczęsny – wziął udział w panelu poprzez połączenie zdalne.

O nowoczesnych technologiach

Temat technologii w biznesie i w codziennym życiu pojawił się drugiego dnia zjazdu. O zastosowaniach internetu rzeczy opowiedział między innymi Jacek Sekuła z polskiej firmy Grenton.

– Oferowany przez nas system Smart Home to rozwiązanie spod szyldu domowej automatyki. Wielu klientów wciąż nie wie, że nowoczesne technologicznie rozwiązania są dostępne, a ich ceny są przystępne – wskazał ekspert.

Goście przybywają!

Pora na nagrody!


Była też chwila na chill


Atmosfera dopisała


Gala trwała do białego rana...

Dowiódł także, że rozwiązania Smart Home to bardzo dynamiczny rynek, w którym swoją niszę (i zarobek) mogą znaleźć także mali i średni operatorzy.

– 10 proc. realizowanych obecnie inwestycji w budownictwie oferuje rozwiązania Smart Home – podkreślił. – Szacuje się też, że kolejny wzrost nastąpi już wkrótce. Warto wiedzieć, że marka Grenton tworzona jest przez byłych członków MiŚOT – dodał.

Wieści z Grupy MiŚOT

Podczas zjazdu duża prezentacja poświęcona była także projektom Grupy MiŚOT. Krzysztof Czuszek zapowiedział między innymi wymianę urządzeń w EPIX-ie oraz stworzenie ringu łączącego wszystkie trzy należące do Grupy MiŚOT węzły wymiany ruchu (Katowice, Warszawa i Poznań).

Tomasz Brol opowiedział natomiast o rozwoju projektu Polska LoRaWAN w każdym powiecie. Inicjatywa jest realizowana na podstawie lokalnego potencjału MiŚOT. Bieżący rok ma być dla polskiego LoRaWAN momentem przełomowym. Twórcy projektu – Krzysztof Czuszek, Sebastian Kachel, Artur Tomaszczyk i Tomasz Brol – przedstawili kalendarium przedsięwzięcia i jego możliwe komercyjne zastosowania. Warto przy tym zaznaczyć, że LoRaWAN w Polsce powstaje na bazie IPV6. Uzasadnienie dla tego rozwiązania przedstawił Artur Tomaszczyk podczas prezentacji IPV4 czy IPV6? Oto jest pytanie….

Mali i średni operatorzy telekomunikacyjni są odpowiedzialni społecznie. O tym opowiedzieli Sebastian Kachel, Paweł Gniadek i Daniel Piecuch. Podkreślili, że dzięki CSR firmy MiŚOT-ów mogą budować relacje z otoczeniem, integrować załogę oraz dbać o ochronę lokalnych terenów i środowiska naturalnego. Podczas uroczystej gali w pierwszym dniu zjazdu wręczono także nagrody w konkursie TeleOdpowiedzialny Roku 2021.

Prężnie rozwija się także MiŚOT Akademia, czyli rozwiązanie przygotowane z myślą o zarządcach firm, którzy wiedzą, że siłą biznesu są dobrze wyedukowani i nadążający za najlepszymi standardami pracownicy i właściciele. MiŚOT Akademia ma za zadanie zapewnić właśnie taki szeroki pakiet szkoleń.

– Siłą MiŚOT-ów jest również lokalność – podkreślał między innymi Marcin Orocz podczas prezentacji odnowionej inicjatywy Lokalni.pl.

Zaprezentowane zostały także inne ważne projekty Grupy: TeleCentrum, MdO i sklep. Zarząd przedstawił informacje o poziomie zaawansowania tworzenia Grupy MiŚOT – skonsolidowanej struktury firm pracujących na rzecz operatorów, kończącym się procesie rejestracji zmian w statucie spółki MiŚOT SA oraz kryteriach udostępnienia operatorom akcji tego podmiotu. – To będzie spółka należąca do operatorów i pracująca dla operatorów – mówił Krzysztof Czuszek. Akcjonariuszami podmiotu będą osoby upoważnione z firm, które korzystają z usług Grupy MiŚOT.

Warto też podkreślić, że wielu uczestników Zjazdu MiŚOT nastawiło się przede wszystkim na indywidualne spotkania i rozmowy. Lokalne spotkania w małym gronie to w przekonaniu organizatorów optymalna i bezpieczna formuła. Kolejne Zjazdy MiŚOT planowane są w 2022 roku i zorganizowane będą w następujących rejonach: Centrum, Wschód i Północ. Ich zwieńczeniem będzie ogólnopolska konferencja.

Cyberbezpieczne MiŚOT-y

Organizatorzy podkreślili kluczowe znaczenie cyberbezpieczeństwa. Maciej Linscheid i Marcin Zemła, eksperci w dziedzinie związani z projektem MiŚOT dla Security, przedstawili przodujące zagadnienia oraz przedstawili, w jaki sposób MiŚOT-y i ich klienci mogą być cyberbezpieczni dzięki rozwiązaniom oferowanym przez Grupę MiŚOT i projekt MdS. Na slajdach zaprezentowane zostały między innymi, zapowiadane w Bukowinie, screeny z interfejsu użytkownika.

Ochrona infrastruktury telekomunikacyjnej to jednak przede wszystkim praktyka. Zadaniem ekspertów było zwrócenie uwagi na potencjalne zagrożenia i metody ich eliminacji, a uczestnicy zjazdu poznali znaczenie testów penetracyjnych i stres testów.

Omawianej tematyki dotknęła też prelekcja o bezpieczeństwie informacji w zderzeniu z konkurencją. Marcin Zemła z pasją opowiedział o trollingu i kształtowaniu rzeczywistości przez korporacje oraz podał kilka skutecznych metod, jak radzić sobie z biznesowymi rywalami wykorzystującymi nieuczciwe zagrywki.

Teraz Kołobrzeg

– Lokalny Zjazd MiŚOT w Janowie Podlaskim pokazał, jak dużą popularnością cieszą się merytoryczne prelekcje dotyczące spraw małych i średnich operatorów – zaznacza Krzysztof Fujarski z projektu MdM, operatora zjazdu. – Podczas wielu z nich obłożenie sal było bliskie 100%, a dyskusje (szczególnie ostatnia) spowodowały, że trzeba było wydłużać czas. Nic dziwnego, że zarówno w Bukowinie, jak i w Janowie Podlaskim zabrakło wejściówek na długo przed końcem rejestracji – dodaje.

Uwielbiana przez MiŚOT-y formuła spotkania na żywo dopiero po raz drugi powróciła w pełnym wymiarze po pandemii. Nie zabrakło dyskusji w przerwach między prelekcjami oraz w kuluarach podczas wieczornej gali. Zjazdy MiŚOT, oprócz przekazywania wiedzy, sprzyjają nawiązywaniu relacji biznesowych. Aktywność uczestników w tym zakresie była znaczna, co w rozmowach z nami potwierdzali też wystawcy. Organizatorzy zapowiedzieli, że kolejne spotkania będą kontynuowały ten trend.

Przypominamy, że kolejny Lokalny Zjazd MiŚOT „Północ" planowany jest na 14–15 czerwca w Kołobrzegu, a zjazd „Zachód" na listopad. Ich organizatorami, podobnie jak w przypadku wydarzenia w Janowie Podlaskim, będą: Grupa MiŚOT, KIKE i Fundacja Nasza Wizja. ■

Polecamy pospieszyć się z rejestracją, zanim zabraknie miejsc. Przypominamy link do rejestracji:

http://misot.pl/zjazdy

KONFERENCJA KIKE 2022

KIKE | MiSOT GRUPA | nasza wizja

Największe spotkanie branży telekomunikacyjnej

19-21 września 2022
Hotel DoubleTree by Hilton, Łódź

Akredytacje w promocyjnej cenie tylko do końca czerwca!
Zarejestruj się już dziś!
Wejdź na stronę
www.KonferencjaKike.pl

Zapraszamy
KIKE | Grupa MiŚOT | Fundacja Nasza Wizja

LUDZIE GRUPY MiŚOT – CZYLI CI, KTÓRZY PRACUJĄ DLA WAS:

Magdalena Drozdowska – kobieta wielu aktywności

KLAUDIA WOJCIECHOWSKA

Na rzecz MiŚOT-ów pracują specjaliści w różnych dziedzinach. Osoby o różnych umiejętnościach, których połączyła praca. A jednocześnie wielu z nich także w czasie wolnym oddaje się swoim pasjom, przez co są jeszcze bardziej fascynujący. Tak samo jest w przypadku Magdaleny Drozdowskiej, dyrektorki biura zarządu Grupy MiŚOT.

Magdalena Drozdowska jako absolwentka ekonomii ze specjalnością analityk rynku na Uniwersytecie Ekonomicznym w Katowicach trafiła do e-Południa już w 2014 roku.

– Kiedy rozpoczęłam pracę w Stowarzyszeniu, był to mój pierwszy zawodowy kontakt z branżą telekomunikacyjną. Wtedy Stowarzyszenie nie prowadziło tak wielu różnych projektów, a moje obowiązki skupiały się wokół EPIX-a. Z biegiem czasu poznawałam branżę, dzięki czemu byłam zaangażowana w nowe zadania i miałam przyjemność nie tylko obserwować, ale też brać udział w rozwoju Stowarzyszenia i powstawaniu Grupy MiŚOT.

Magdalena jest dyrektorką biura zarządu. Zajmuje się organizacją pracy biura Grupy MiŚOT SA tak, by sprawnie funkcjonowało. W obrębie jej zadań są sprawy związane z pracownikami Grupy i jej kontrahentami oraz innymi instytucjami. Na co dzień pozostaje też w stałym kontakcie z kancelariami księgowymi oraz prawnymi obsługującymi Grupę.

– Pracuję w biurze w Bytomiu wraz z małym zespołem. Tworzył się on stopniowo u mojego boku wraz z przybywającą liczbą przedsięwzięć grupy MSA. W naturalny sposób rósł on wraz ze Stowarzyszeniem. Kolejne ręce do pomocy przybywały stopniowo w miarę, jak pojawiały się nowe projekty i istniejącemu zespołowi przybywało nowych obowiązków. A te obowiązki są bardzo różnorodne i trzeba być wszechstronnym, by im sprostać. Czasem trzeba też robić kilka rzeczy naraz i żadna z nich nie jest ważniejsza lub mniej istotna. Musimy sprawnie i szybko reagować, chociażby w sytuacji, gdy redagujemy maila do MiŚOT-a w sprawie OSE, a w tym czasie zadzwoni klient e-Południa w sprawie płatności. Obie sprawy załatwia się właściwie jednocześnie.

Jak widać, Stowarzyszenie rozrastało się i zmieniało na oczach swojej dyrektorki biura. Uczestniczyła ona także w działaniach Projektu MdO w ramach OSE.

– Można powiedzieć, że Projekt OSE był na samym początku białą kartką, którą stopniowo zapisywaliśmy. Pamiętam pierwszy przetarg OSE organizowany przez NASK, w którym Projekt MdO startował w imieniu MiŚOT-ów. Nasza oferta miała w sumie z załącznikami kilkadziesiąt stron, większość danych wpisywana była ręcznie, a cała procedura wydawała się mocno skomplikowana. Po sukcesie MdO w tym pierwszym przetargu obsługa pierwszych uruchomionych lokalizacji również wymagała dużo pracy bezpośredniej, takiej jak kontakty z MiŚOT-ami – opowiada o początkach MdO Magdalena. – Po doświadczeniach z pierwszego i kolejnych przetargów stopnio-

wo były wyłapywane elementy, które mogły zostać zautomatyzowane. Dzięki temu teraz jest możliwe obsłużenie ponad trzech tysięcy uruchomionych lokalizacji przy udziale stosunkowo niewielkiego zespołu.

Ale Magdalena Drozdowska nie tylko zawodowo jest bardzo aktywna i łączy różne umiejętności i wykonywanie różnorodnych zadań. W życiu prywatnym jest tak samo. Aż trudno uwierzyć, że jedna osoba może mieć tyle pasji i oddawać się im z takim zaangażowaniem.

– Prywatnie jestem bardzo aktywną osobą, miłośniczką podróżowania. Ale nie takiego z biurem podróży, tylko organizowanego na własną rękę. Najlepiej bym się czuła, gdybym na urlopie każdego dnia znajdowała się w innym miejscu. Tak w Polsce, jak i za granicą.

W opowieściach o podróżach pojawia się również rower. Ale nie jest to rower miejski i wypady na zakupy czy podróż do pracy. To wielodniowe wyprawy z sakwami. Rower jako pojazd wyjazdowy? Dlaczego nie?

– W ten sposób zwiedziłam chyba już całą Polskę, prawie całą Holandię, troszkę Węgry i Czechy. Moim rowerowym wyczynem jest przejechanie na rowerze crossowym (nie na szosie, co stanowi różnicę) 200 km w czasie poniżej 10 godzin – opowiada Magdalena. – Podróżowanie rowerem ma tę przewagę, że pozwala łączyć w sobie aktywność, przebywanie na świeżym powietrzu i dodatkowo możliwość przemieszczania się. Rowerem można przemierzać tereny, gdzie innymi środkami lokomocji nie dałoby się dojechać – może udałoby się jedynie pieszo, ale znów dzienny dystans, jaki można pokonać rowerem, jest większy niż pieszo. Z tego względu rower zaspokaja te wszystkie potrzeby podróżnika, których moim zdaniem siedzenie przy basenie nigdy by nie zaspokoiło. Aktywny wypoczynek jest może nie tyle odreagowaniem pracy biurowej, co chęcią zmiany otoczenia z pokoju biurowego i mieszkania w mieście na duże przestrzenie i bliskość natury.

Podczas planowania wypraw ze szczególnym zainteresowaniem patrzy w stronę gór. Zdobyła Koronę Gór Polski, co jest niemałym wyczynem. A wszystko zaczęło się na studiach.

– Zaplanowałam sobie wtedy urlop, w czasie którego miałam przejść od Równicy do Babiej Góry, cały czas poruszając się czerwonym szlakiem i śpiąc w schroniskach PTTK po drodze. To była niezapomniana do dziś przygoda, podczas której powstały kolejne i kolejne plany na wędrówki w przyszłości.

Swoje pasje sportowe i podróżnicze Magdalena dzieli z narzeczonym. Oboje lubią aktywny wypoczynek i w takich też okolicznościach się poznali. Ale to już zupełnie inna historia.. ■

Magdalena Drozdowska nie tylko zawodowo jest bardzo aktywna i łączy różne umiejętności i wykonywanie różnorodnych zadań. W życiu prywatnym jest tak samo. Aż trudno uwierzyć, że jedna osoba może mieć tyle pasji i oddawać się im z takim zaangażowaniem.

CO OZNACZA STAN WYJĄTKOWY DLA OPERATORÓW?

MAREK NOWAK

Choć wciąż wszyscy liczymy na zakończenie działań wojennych podjętych przez Rosję wobec Ukrainy, warto rozważyć mniej optymistyczne scenariusze.

– W przypadku nasilenia się wojny w Ukrainie możliwym scenariuszem dla Polski wydaje się wprowadzenie stanu wyjątkowego – mówi Ilona Malik, radczyni prawna współpracująca z Grupą MiŚOT.

Stan wyjątkowy jest jednym ze stanów nadzwyczajnych wyróżnionych w Konstytucji Rzeczypospolitej Polskiej obok stanu wojennego oraz klęski żywiołowej. Szczegółowe kwestie dotyczące wprowadzenia stanu wyjątkowego reguluje ustawa o stanie wyjątkowym. Dopuszcza ona wprowadzenie wielu ograniczeń, które wpływają na prowadzenie biznesu, w tym odnoszących się bezpośrednio do branży telekomunikacyjnej – dla przykładu: dotyczących kontroli treści korespondencji telekomunikacyjnej lub sygnałów przesyłanych w sieciach telekomunikacyjnych, zagłuszania nadawania lub odbioru przekazów dokonywanych poprzez urządzenia i sieci telekomunikacyjne, funkcjonowania systemów łączności oraz działalności telekomunikacyjnej.

Należy również wspomnieć o restrykcjach, które mogą być wprowadzone i wpływają na prowadzenie każdego biznesu bez względu na branżę, jak np. zakaz okresowego podwyższania cen na towary lub usługi określonego rodzaju albo wręcz nakazanie stosowania określonych cen, ograniczenie obrotu krajowymi środkami płatniczymi, obrotu dewizowego oraz działalności kantorowej, nakaz okresowego zaniechania prowadzenia działalności gospodarczej określonego rodzaju, ograniczenia transportu drogowego, kolejowego i lotniczego oraz w ruchu morskim i śródlądowym.

Zadania i obowiązki

Z jednej strony mamy ograniczenia i restrykcje, z drugiej strony wiele zadań i obowiązków nałożonych na przedsiębiorców ustawą Prawo telekomunikacyjne oraz innymi przepisami. Przedsiębiorca telekomunikacyjny w sytuacjach szczególnego zagrożenia zobowiązany jest do ścisłej współpracy z takimi podmiotami jak Straż Pożarna, Straż Graniczna, Policja, ABW, organy administracji rządowej i samorządowej, szpitale.

Jego obowiązkiem jest:

- zapewnienie dostępu i możliwości utrwalania przekazów telekomunikacyjnych i danych towarzyszących na rzecz sądów i prokuratury;
- nieodpłatne udostępnianie urządzeń telekomunikacyjnych,
- blokowanie ruchu telekomunikacyjnego.

Ponadto Rada Ministrów, mając na uwadze zakres i rodzaj wykonywanej działalności gospodarczej, wielkość przedsiębiorcy telekomunikacyjnego i jego znaczenie dla gospodarki, obronności, bezpieczeństwa państwa oraz porządku publicznego, w drodze rozporządzenia narzuca obowiązek sporządzania i aktualizowania planów działania w sytuacjach szczególnego zagrożenia.

Z obowiązku sporządzenia tych planów zwolnieni są przedsiębiorcy, których roczny dochód z tytułu wykonywania działalności telekomunikacyjnej w poprzedzającym roku był równy lub mniejszy niż 10 mln złotych lub którzy, dla przykładu, świadczą usługi wyłącznie polegające na udogodnieniach towarzyszących lub obejmujące zakresem teren nie większy niż powiat (z wyłączeniem miast powiatowych), dostarczają wyłącznie sieć lub łącze telekomunikacyjne dzierżawione od innych przedsiębiorców, nie posiadają własnej sieci telekomunikacyjnej i usługi świadczą, korzystając z sieci innego przedsiębiorcy telekomunikacyjnego, a ich usługi polegają wyłącznie na zapewnieniu dostępu do internetu za pośrednictwem sieci telekomunikacyjnej obsługującej do 1000 zakończeń sieci posiadających własny adres IP.

– To tylko część przykładów ograniczeń i obowiązków nakładanych na przedsiębiorców telekomunikacyjnych, które w sposób znaczący wpływają na prowadzony biznes – zaznacza Ilona Malik. – Pamiętajmy jednak, że wprowadzenie stanów nadzwyczajnych jest możliwe tylko w sytuacji szczególnego zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, w tym spowodowanego działaniami o charakterze terrorystycznym lub działaniami w cyberprzestrzeni, które nie może być usunięte poprzez użycie zwykłych środków konstytucyjnych.

Procedura wprowadzenia stanu wyjątkowego jest także ściśle sformalizowana, a zasady działania organów władzy publicznej oraz zakres, w jakim mogą zostać wprowadzone ograniczenia i restrykcje, a także podstawy, zakres i tryb wyrównywania strat majątkowych, musi regulować ustawa. Warto przy tym zaznaczyć, że rekompensata strat majątkowych nie jest obligatoryjna, a w doktrynie często pojawia się w tym kontekście określenie obowiązku politycznego (moralnego) względem obywateli, nie zaś prawnego.

Lokalnie lub w całym kraju

Stan wyjątkowy może zostać wyprowadzony zarówno na wybranym obszarze, jak i na terenie całego kraju, na czas oznaczony, nie dłuższy niż 90 dni. Przedłużenie stanu wyjątkowego może nastąpić tylko raz, za zgodą Sejmu i na czas nie dłuższy niż 60 dni.

W ostatnim czasie stan wyjątkowy wprowadzono we wrześniu 2021 r. we wschodniej Polsce przy granicy z Białorusią w związku z kryzysem migracyjnym – na obszarze części województwa podlaskiego oraz części województwa lubelskiego. ■

NOWY PROJEKT USTAWY O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

Co się zmieniło w obowiązkach przedsiębiorców telekomunikacyjnych nałożonych w UKSC i jak przygotować do zmian swoją firmę?

MARTA HERÓD, RADCA PRAWNY W KANCELARII PRAWNEJ BRIGHTSPOT

15 marca 2022 r. opublikowano nowy projekt ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (dalej jako UKSC). Jest to temat bardzo aktualny w kontekście obecnej sytuacji na świecie, zwłaszcza rosnącej liczby cyberataków.

W niniejszym artykule wyjaśnię, jak nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa wpływa na działanie firm telekomunikacyjnych. Ustawodawca nie oszczędza bowiem operatorów telekomunikacyjnych, jeśli chodzi o nakładane obowiązki regulacyjne, dlatego pokażę, jakie nowe wyzwania stoją przed branżą telco i jak się do nich przygotować.

Przedsiębiorca telekomunikacyjny pozostaje częścią krajowego systemu cyberbezpieczeństwa

Najistotniejszym z punktu widzenia branży telco założeniem projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa z dnia 15 marca 2022 r. jest włączenie przedsiębiorców komunikacji elektronicznej (obecnych przedsiębiorców telekomunikacyjnych w rozumieniu ustawy Prawo telekomunikacyjne) do grona podmiotów objętych krajowym systemem cyberbezpieczeństwa. Oznacza to konieczność dostosowania się do wymogów ustawy o krajowym systemie cyberbezpieczeństwa oraz sprostania nowym obowiązkom.

Obecny projekt zakłada włączenie do ustawy całego podrozdziału poświęconego obowiązkom przedsiębiorców telekomunikacyjnych. Jest to istotna zmiana wobec projektu z października 2021 r., kiedy to zasadą było nie stosowanie zapisów UKSC wobec przedsiębiorców telekomunikacyjnych z paroma wyjątkami, a kwestia bezpieczeństwa sieci była mocniej opisana w projekcie ustawy Prawo komunikacji elektronicznej.

Mimo tej zmiany obowiązki z zakresu szeroko rozumianego bezpieczeństwa sieci nadal będą jednak znajdować się w różnych aktach prawnych. O ile bowiem UKSC uchyla dział VIIA Prawa telekomunikacyjnego traktujący o bezpieczeństwie i integralności sieci, o tyle ustawodawca pozostawił (jak na razie w projekcie ustawy Prawo komunikacji elektronicznej) zapisy dotyczące zadań wykonywanych na rzecz obronności. Zasady z zakresu bezpieczeństwa i zasady z zakresu obronności w pewnym stopniu krzyżują się – powinny być one więc uregulowane w jednym akcie prawnym dla zachowania czytelności i jasności tych przepisów. W przyszłości może bowiem powstać wiele wątpliwości interpretacyjnych w zakresie tego, które przepisy są ważniejsze i które należy stosować w pierwszej kolejności. Na razie jednak opublikowane projekty kontynuują ten podział – a zatem też stwarzają dalsze ryzyko niejasności.

Incydenty znane z RODO a incydenty telekomunikacyjne

Pojęcie incydentu znane jest operatorom telekomunikacyjnym z RODO. Po wejściu w życie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa operator będzie musiał identyfikować i zapewniać obsługę tzw. incydentów telekomunikacyjnych. Są to jednak różne incydenty – ten z RODO dotyczy naruszenia danych osobowych, ten drugi dotyczy zdarzenia, które ma **rzeczywisty, niekorzystny skutek dla bezpieczeństwa sieci i usług komunikacji elektronicznej**. Takim zdarzeniem będzie cyberatak w każdej postaci – wycieki danych, ataki DDOS, ataki malware, spyware, botnety, ransomware czy ataki socjotechniczne.

Operator będzie zobowiązany do obsługi tych incydentów, czyli do podejmowania czynności zmierzających do wykrycia zdarzenia skutkującego naruszeniem bezpieczeństwa sieci, podjęcia odpowiednich działań naprawczych oraz ograniczenia negatywnych skutków tego incydentu. Jeżeli operator stwierdzi przesyłanie komunikatów, które zagrażają jego sieci, będzie on mógł zablokować przesłanie tego komunikatu, a nawet ograniczyć lub przerwać świadczenie usług (oczywiście do czasu ustania stanu zagrożenia i w celu zapobiegnięcia zagrożeniu).

W przypadku gdy stosowane przez Państwa obecnie regulaminy świadczenia usług telekomunikacyjnych nie zawierają szczegółowych zapisów o możliwości blokowania przesyłania komunikatów ze względu na treść przepisów prawa – warto pamiętać o zawarciu w przyszłości odpowiedniego postanowienia w regulaminie świadczenia usług telekomunikacyjnych.

Każdy stwierdzony incydent telekomunikacyjny będzie musiał być zarejestrowany, **a ten uznany za poważny (rozporządzenie wykonawcze ma określać dokładnie, co to oznacza poważny incydent) będzie podlegał m.in. zgłoszeniu do CSIRT Telco niezwłocznie, nie później jednak niż w ciągu 24 godzin od momentu jego wykrycia**. W zasadzie nie trudno to zapamiętać, bo dokładnie tyle samo czasu mają przedsiębiorcy telekomunikacyjni na zgłoszenie incydentu związanego z zagrożeniem naruszenia danych osobowych. Obok zawiadomienia do CSIRT Telco, jeżeli wpływ

incydentu na dostępność usługi zostanie zakwalifikowany przez samego operatora jako istotny, konieczne będzie zawiadomienie o incydencie abonentów. Informację taką będzie można publikować na stronie internetowej.

Zgłoszenie o wystąpieniu poważnego incydentu będzie musiało zawierać szczegółowy opis jego stwierdzenia oraz jego wpływu na sieć telekomunikacyjną, usługi czy wykonywanie zadań z zakresu obronności. Dobra wiadomość jest taka, że jeśli pewnych danych nie zostaną zgłoszone od razu, będzie można je uzupełnić.

Żeby rejestrowanie incydentów i ich obsługa była efektywna, konieczne będzie przygotowanie nowych procedur w firmie, na które będą składały się formularze zgłoszenia incydentu, procedury ich wysyłki do odpowiednich organów czy umieszczenia odpowiednich danych na swojej stronie internetowej.

Przygotuj swoją stronę internetową pod nowe obowiązki

Obok klasycznych już informacji na stronie www, takich jak np. w polityce prywatności, polityce cookies, regulaminach i cennikach, operatorzy będą musieli umieszczać informacje o:

❶ potencjalnych zagrożeniach związanych z korzystaniem przez abonentów z usług komunikacji elektronicznej;

❷ rekomendowanych środkach ostrożności i najbardziej popularnych sposobach zabezpieczania telekomunikacyjnych urządzeń końcowych przed oprogramowaniem złośliwym lub szpiegującym;

❸ przykładowych konsekwencjach braku lub nieodpowiedniego zabezpieczenia telekomunikacyjnych urządzeń końcowych.

Wydaje się, że informacje te będą musiały być niezależnie wyodrębnione od innych dokumentów i informacji na stronie www operatora, nawet jeśli te informacje będą umieszczone bezpośrednio, np. w regulaminie opublikowanym na stronie www. Operatorów czeka zatem przygotowanie strony internetowej pod nowe obowiązki – obok polityk prywatności powinny się bowiem znaleźć informacje o cyberbezpieczeństwie.

Jeżeli incydent telekomunikacyjny będzie tym poważnym incydentem – przedsiębiorca komunikacji elektronicznej będzie zobowiązany opublikować na swojej stronie internetowej także informację o wystąpieniu poważnego incydentu telekomunikacyjnego w terminach wynikających z UKSC.

Plany szczególnych zagrożeń

Przedsiębiorca telekomunikacyjny, który sporządza na podstawie przepisów branżowych plany szczególnych zagrożeń (jest do tego zobowiązany), będzie musiał w nich zawrzeć dodatkowe informacje wynikające z UKSC. Ci operatorzy, na których nie spoczywa obowiązek sporządzenia planu, będą musieli konkretne czynności udokumentować. Do tych czynności i informacji zaliczyć należy dokonywanie regularnych ocen ryzyka wystąpienia sytuacji szczególnego zagrożenia, a także stosowane środki zabezpieczeń przed naruszeniem bezpieczeństwa sieci mające wpływ na sieć czy świadczenie usług telekomunikacyjnych.

Operatorzy, którzy założyli, że zwolnienie ich z obowiązku sporządzenia planów szczególnego zagrożenia skurczy chociaż trochę obowiązki, które do nich należą, są w błędzie. Będą oni i tak zobowiązani do przygotowania planów – roboczo przeze mnie nazywanych planami ochrony przed cyberzagrożeniami.

CSIRT Telco może dokonywać oceny bezpieczeństwa systemu informacyjnego operatorów telekomunikacyjnych, w tym w sposób pozwalający na przełamywanie zabezpieczeń sieci.

CSIRT Telco będzie mogło przeprowadzić ocenę bezpieczeństwa systemu informacyjnego przedsiębiorcy komunikacji elektronicznej za zgodą właściwego CSIRT GOV, CSIRT MON lub CSIRT NASK. Co istotne, CSIRT Telco będzie mogło używać urządzeń i programów co do zasady zakazanych na gruncie kodeksu karnego, a zmierzających do nieuprawnionego dostępu do danych w sieci telekomunikacyjnej. W ten sposób legalne będzie uzyskanie przez zespół CSIRT Telco dostępu do informacji dla niego nieprzeznaczonych – poprzez przełamanie albo ominięcie elektronicznego, magnetycznego, informatycznego lub innego szczególnego jej zabezpieczenia. Możliwe również będzie uzyskanie dostępu do całości lub części systemu teleinformatycznego przez CSIRT Telco.

Oczywiście dane te będą traktowane jako tajemnice prawnie chronione i nie będą mogły być wykorzystane do celów innych niż ocena bezpieczeństwa systemów operatorskich. Dane pozyskane w ramach dokonywania tejże oceny będą niszczone po ich uzyskaniu.

Dostawcy usług i produktów uznani za dostawców wysokiego ryzyka

Przedsiębiorcy telekomunikacyjni zostali de facto pozbawieni udziału w postępowaniach dotyczących uznania dostawców usług i produktów ICT za dostawców wysokiego ryzyka. W postępowaniach tych udział w charakterze strony będzie możliwy – poza badanym dostawcą – dla przedsiębiorców telekomunikacyjnych, których przychód z tytułu prowadzenia działalności telekomunikacyjnej odpowiada co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej (na chwilę obecną w przybliżeniu 110 milionów złotych).

Mali i średni przedsiębiorcy telekomunikacyjni nie osiągają przychodów w powyższej wysokości – mówimy zatem o ograniczeniu prawa do udziału w postępowaniu do dużych telekomów – ISP zostali jawnie pozbawieni tego prawa. Co to oznacza dla małych i średnich przedsiębiorców? Nie będą oni mogli sprzeciwić się na żadnym etapie uznawania dostawców usług czy produktów ICT za dostawców wysokiego ryzyka i zmuszeni będą do wycofania określonych typów produktów czy usług ICT, z których korzystają w swojej działalności.

Podsumowując, operatorzy telekomunikacyjni powinni przygotować się do wdrożenia kolejnych planów na wypadek wystąpienia cyberzagrożeń i przygotować swoje firmy (ale też pracowników) do obsługi incydentów telekomunikacyjnych. Prace nad nowelizacją UKSC ruszyły ponownie i można się spodziewać, że już niedługo UKSC wejdzie w życie. ■

Jeżeli temat cyberbezpieczeństwa Państwa zainteresował, zapraszamy do kontaktu pod adresem info@brightspot.pl lub pod numerem telefonu 12 311 04 42.

LEX HUAWEI, CZYLI KTO SIĘ BOI KSC?

MAREK NOWAK

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy Prawo telekomunikacyjne doczekał się już aż siedmiu wersji. Ostatnia z nich opublikowana była w marcu. Dyskusja o obawach operatorów związanych z zapisami projektu powróciła jednak na Lokalnym Zjeździe MiŚOT w Janowie Podlaskim.

Już pierwszy projekt zmian w ustawie o krajowym systemie cyberbezpieczeństwa wzbudził w środowisku małych i średnich operatorów telekomunikacyjnych ogromne kontrowersje. Był też szeroko omawiany i krytykowany podczas konsultacji społecznych czy Wirtualnego Kongresu Przedsiębiorców Telekomunikacyjnych. Druga, trzecia i kolejne wersje projektu nie były już z nikim konsultowane, pomimo postulatów zgłaszanych w tej sprawie przez organizacje branżowe.

– Biorąc pod uwagę całą historię tych wszystkich poprawek do ustawy o zmianie ustawy o KSC, ciężko nie oprzeć się wrażeniu, że nasz rząd buduje narzędzie do wewnętrznych rozgrywek rynkowych promujących duże firmy telekomunikacyjne oraz usiłuje tylnymi drzwiami wprowadzić cenzurę pod dowództwem politycznym w świat internetu – mówi Marcin Zemła z projektu MiŚOT dla Security (MdS). – Zarówno zapisy dotyczące dostawcy wysokiego ryzyka, jak i uznaniowe wprowadzanie blokad treści po opublikowaniu przez Prezesa Rady Ministrów listy adresów IP do zablokowania niosą ze sobą pełną uznaniowość tych czynności. Brak jakichkolwiek przesłanek technologicznych lub drogi poprawy – dodaje.

Największe emocje i niepokoje budzą wśród małych i średnich operatorów telekomunikacyjnych konsekwencje uznania przez właściwego ministra do spraw informatyzacji (według stanu obecnego – premiera) określonego dostawcy sprzętu za dostawcę wysokiego ryzyka, stanowiącego „poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi. Sprzęt takiego dostawcy trzeba będzie w ciągu siedmiu lat wycofać z użytku (w przypadku gdy wchodzi on w skład infrastruktury krytycznej – w ciągu pięciu lat).

– Przeraża mnie uznaniowość decyzji dotyczącej tego, który producent sprzętu jest poprawny politycznie, a który nie – zaznacza Joanna Macek-Czuszek, prezeska firmy ART-COM z Jaworzna. – Nie mamy przecież gwarancji, czy po jakimś czasie inny producent nie popadnie w niełaskę i całą operację trzeba będzie powtarzać.

Sytuacja na rynku

Ponieważ wiodący dostawca sprzętu telekomunikacyjnego dla małych i średnich operatorów jest jeden, nowelizację ustawy o KSC część komentatorów nazywać zaczęła mianem Lex Huawei. Określenie to nie tyle jednak upraszcza, ale wręcz deformuje spojrzenie na przygotowywane przepisy. Nie bierze ono pod uwagę sytuacji panującej obecnie na rynku sprzętu telekomunikacyjnego w Europie i na świecie.

– Zgodnie z protestem Huawei prawo powinno dopuszczać możliwość przywrócenia na rynek sprzętu po uwzględnieniu poprawek – podkreśla Marcin Zemła. – To logiczny argument, nie uwzględniony jednak w treści ustawy. Dokładnie taka sama sytuacja jest z blokowaniem treści i adresów. Rekomendacje przewidzianego w przepisach Komitetu nie są sprecyzowane i nie wiadomo, na podstawie jakich kryteriów ta ocena ma się odbywać. Co więcej, jest to ocena ostateczna. Wprowadzenie tych przepisów daje duże możliwości lobbowania pewnych działań, a rządowi pozwala tylnymi drzwiami wprowadzać polityczną cenzurę, w zasadzie bez jasnych przesłanek, na zasadzie: Komitet uznał i tak ma być.

Warto też zaznaczyć, że firm azjatyckich, od których mali i średni operatorzy telekomunikacyjni kupują sprzęt, jest oczywiście więcej. Często też zawierane są małe kontrakty obejmujące tysiąc czy kilka tysięcy urządzeń. Problemem jest także to, że operatorzy praktycznie nie mają alternatywy w postaci perspektywy handlu z europejskimi firmami.

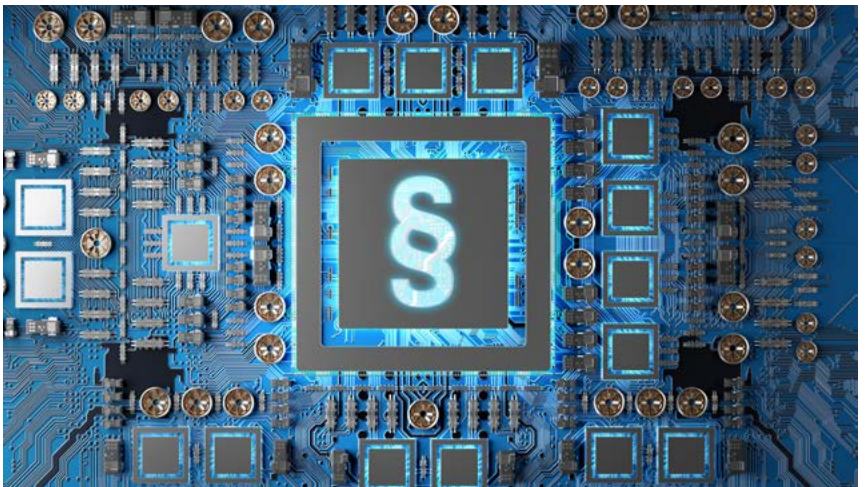
KIKE działa

Krajowa Izba Komunikacji Ethernetowej już dwa lata temu poprosiła MiŚOT-ów o dane na temat kosztów ewentualnej wymiany sprzętu. Należało je przesłać w niezwykle krótkim czasie, aby w ogóle stanowisko małych i średnich operatorów zostało uwzględnione przez ustawodawcę podczas konsultacji z przedstawicielami administracji państwowej. Izba podkreślała wówczas, że nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa grozi bankructwem wielu MiŚOT-ów.

– Kiedy we wrześniu 2020 roku odpowiedzieliśmy na ankietę KIKE dotyczącą kalkulacji kosztów wynikających z potencjalnej konieczności wymiany sprzętu, już pobieżna weryfikacja uzmysłowiła nam, że prawdopodobnie nikt z pomysłodawców ustawy nie analizował jej w tym kontekście – mówi Joanna Macek-Czuszek. – Prowadzona przez nas firma musiałaby w określonym ustawowo czasie przeznaczyć na wymianę sprzętu (według kalkulacji sprzed dwóch lat) ponad pięć milionów złotych. Warto przy tym zaznaczyć, że koszty zakupu nowego sprzętu to tylko jeden z problemów. Kolejnym byłaby dziś jego dostępność, która na skutek pandemii oraz wojny na Ukrainie jest mocno ograniczona. Nie mniej ważny byłby również koszt robocizny związany z wymianą urządzeń – dodaje.

W środowisku dominuje też opinia, że jeśli zmiana producenta sprzętu miałaby okazać się konieczna na skutek wprowadzenia nowych przepisów, powinna być wykonana dopiero w chwili jego naturalnego zużycia, w innych zaś wypadkach koszty tej wymiany powinny obciążyć Skarb Państwa.

Operatorzy konsekwentnie tworzą więc wspólny front, podkreślając, że owe zapisane w projekcie siedem lat w praktyce nic właściwie nie da, a na tytułowe pytanie o strach przed zmianami w ustawie o KSC odpowiedzieć należy, że obawiać się ich powinni wszyscy mali i średni operatorzy telekomunikacyjni. ■



CZY CYBERBEZPIECZEŃSTWO JEST PRETEKSTEM DO CENTRALIZACJI?

MICHAŁ KOCH

Wysoki poziom skomplikowania zadań dotyczących administracji, bezpieczeństwa, a także telekomunikacji skłaniał do tej pory do decentralizacji odpowiedzialnych podmiotów oraz do tworzenia odpowiednich organów bliżej przedmiotu działania. Od jakiegoś czasu obserwujemy jednak zmianę trendu, a w publicznych dyskusjach coraz częściej mówi się o konieczności centralizacji. Czy cyberbezpieczeństwo może być pretekstem do tworzenia kolejnych, zarządzanych przez państwo instytucji?

W projekcie ustawy o krajowym systemie cyberbezpieczeństwa (KSC) znajdziemy pomysł utworzenia Operatora Strategicznej Sieci Bezpieczeństwa. OSSB ma z założenia dbać o cały obszar telekomunikacji w Polsce. Dotyczy to zarówno łączności przewodowej, jak i bezprzewodowej. Jeżeli przepisy KSC staną się częścią polskiego porządku prawnego, to OSSB będzie „meta-operatorem", czyli podmiotem o szerokim zakresie uprawnień i obowiązków, świadczącym różnego rodzaju krytyczne usługi łączności dla wybranych klientów (w tym dla państwa), niezależnie od użytej technologii.

Wydarzenia ostatnich kilku lat, w tym najnowsze cyberataki na strony internetowe instytucji rządowych w Europie, pokazują, że cyberbezpieczeństwo to ważny, o ile nie najważniejszy, problem do rozwiązania. Przepisy KSC miały za zadanie przygotować telekomunikacyjną infrastrukturę w Polsce do zarządzania cyberbezpieczeństwem oraz utworzyć szereg niezbędnych zależności i połączeń, by sprawnie działać m.in. w zakresie obsługi „first responders", czyli użytkowników takich jak straż, policja oraz pogotowie.

Nowe przepisy budzą jednak coraz więcej kontrowersji. Marcin Zemła, reprezentujący projekt MiŚOT dla Security (MdS), jest zdania, że rząd chce stworzyć podmiot do wewnątrzrynkowych rozgrywek, by w rezultacie promować duże firmy telekomunikacyjne. Szerzej o obawach lokalnych operatorów w związku z KSC przeczytacie przeczytacie w artykule Lex Huawei na stronie 36.

Okazuje się, że nie tylko operatorzy mają zastrzeżenia. Uwagi zgłasza też strona rządowa. Wątpliwości Ministerstwa Spraw Wewnętrznych i Administracji dotyczą przede wszystkim sposobu finansowania usług i wydatkowania środków publicznych, który w projekcie ma nie być wystarczająco jasno sformułowany. Pełna transparentność w zakresie finansowym wydaje się kluczowym elementem, by przepisy KSC miały rację bytu.

Głos w dyskusji zabrali członkowie Grupy Bezpieczeństwa GROT w Polskiej Izbie Informatyki i Telekomunikacji (PIIT), która zrzesza polskich operatorów telekomunikacyjnych. Sygnalizują, że w nowelizacji KSC w dalszym ciągu znajdują się zapisy wyłączające stosowanie prawa zamówień publicznych przy zawieraniu przez administrację publiczną umów z operatorem strategicznej sieci bezpieczeństwa. Ich zdaniem spowoduje to powstanie monopolu dla OSSB.

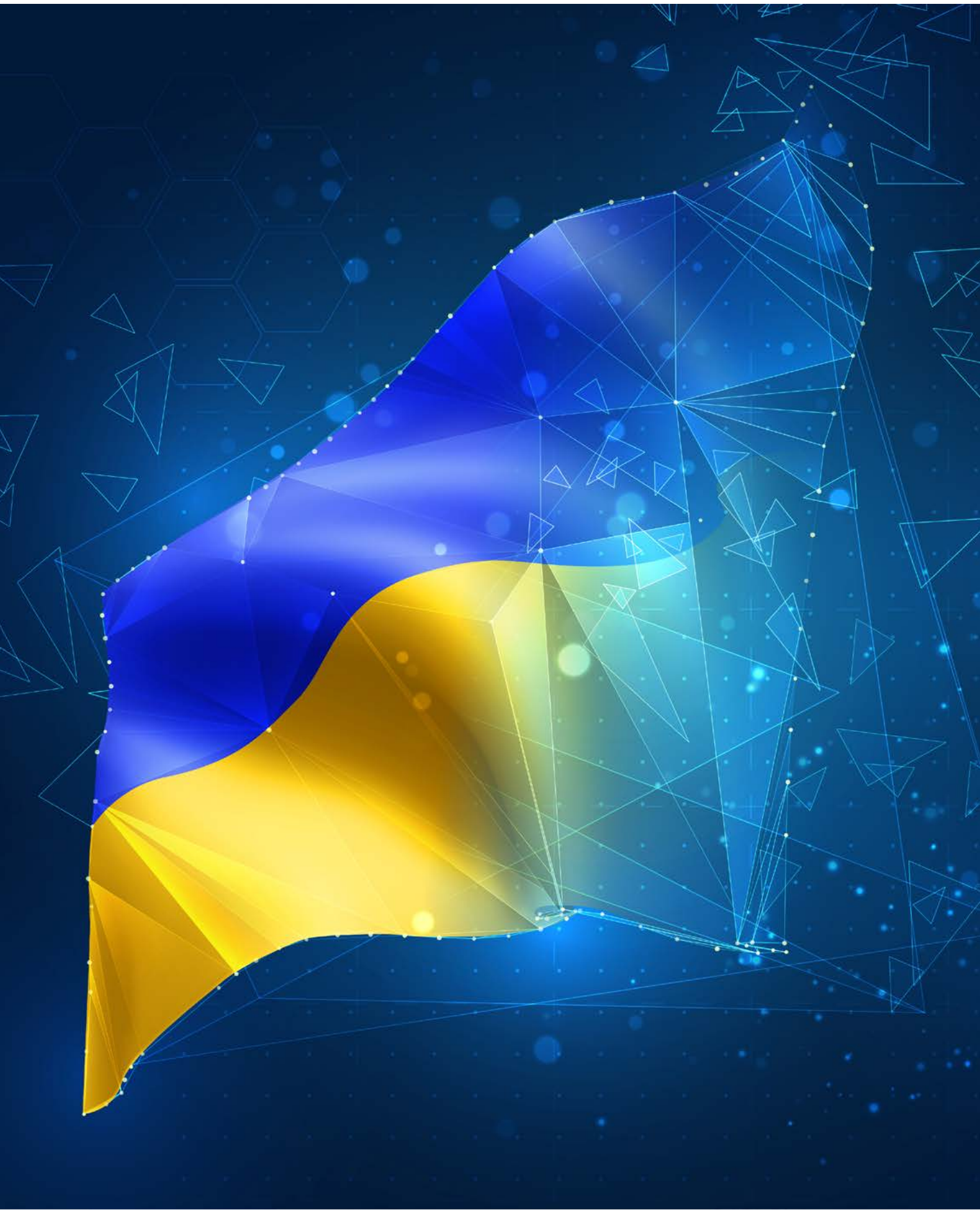
Exatel, czyli państwowy operator telekomunikacyjny i dostawca usług cyberbezpieczeństwa, którego 100 proc. akcji jest w rękach Skarbu Państwa, jest brany pod pod uwagę jako podmiot, który może stać się OSSB. Pomysł napotkał sprzeciw, a wśród zarzutów jest m.in. fakt, że w dyskusji pomijany jest głos mniejszych operatorów, którzy obawiają się marginalizacji wpływu na kształt rynku.

Michał Szczęsny, dyrektor biura architektury i planowania sieci Exatel, jest jednak zdania, iż operatorom nie opłaca się stawiać stacji bazowych na terenach niezamieszkałych i trudno dostępnych. – Operatorzy wolą w tych miejscach nie mieć zasięgu albo wyłącznie taki na poziomie sieci 2G/3G. Rachunek finansowy jest okrutny – przekazał Szczęsny w rozmowie z portalem CyberDefence24.pl. Problem znikającego zasięgu i białych plam łączności miałby więc zostać rozwiązany na poziomie centralnym.

Przedstawiciele Exatela bronią przepisów, KSC, argumentując, iż 99 proc. pokrycia siecią telekomunikacyjną powierzchni kraju odnosi się wyłącznie do populacji, czyli liczby Polaków, którzy znajdują się w zasięgu. Pod kątem geograficznym jest już gorzej. Trudno tu nie przyznać racji (zresztą, kto z nas np. podczas podróży pociągiem nie znalazł się w obrębie tzw. białej plamy zasięgu?), ale utworzenie podmiotu, który miałby niepisane pierwszeństwo na rynku telekomunikacyjnym, zwłaszcza bez konsultacji z krajowymi lokalnymi operatorami, może sprawić, że polski rynek telekomunikacyjny zostanie postawiony na głowie.

W tle jest jeszcze sprawa budowy polskiej sieci 5G. Aukcja bardzo się opóźnia, a świat na nas nie czeka. Spółka #Polskie5G ma być operatorem hurtowym, który buduje zasoby bezprzewodowej łączności w tym standardzie. Ma to pomóc w efektywnym rozdysponowaniu pasma 700 MHz.

Sprawa Krajowego Systemu Cyberbezpieczeństwa i Operatora Strategicznej Sieci Bezpieczeństwa od miesięcy budzi kontrowersje. Powyższe przykłady wskazują, że trwa rozgrywka na kilku instytucjonalnych szczeblach, ale sprawa rozbija się też o prawo prywatnych firm do funkcjonowania na rynku bez nieuczciwej konkurencji. Centralizacja jest czasem dobrym rozwiązaniem, zwłaszcza że tuż obok naszych granic trwa cyberwojna, jednakże nie można zapominać, że rynek telekomunikacyjny w Polsce ma długą tradycję, a mali i średni operatorzy są jego częścią od dawna. Może warto byłoby wysłuchać ich zdania w sprawie cyberbezpieczeństwa. ■



UKRAIŃSKI ŁĄCZNIK

MICHAŁ KOCH

Internet jest bez wątpienia częścią infrastruktury krytycznej każdego kraju. We współczesnym świecie dzięki łączności możemy zrealizować praktycznie wszystkie działania, w tym te dotyczące obronności. Telekomunikacja odgrywa niebagatelną rolę także podczas wojny w Ukrainie. Obrona przed Rosją wymaga zarówno koordynacji konwencjonalnych działań zbrojnych, jak i tych w cyberprzestrzeni.

Ukraina przekształciła się z kraju, w którym koszt internetu jest dla obywatela wysoki, w państwo o przyjaznych i rozsądnych warunkach dostępu do cyberprzestrzeni. Telekomunikacja odegrała tam także ważną rolę w czasie trwania pandemii koronawirusa, a liczba użytkowników sieci w 2021 roku wyniosła ok. 30 mln osób. Rzeczywistość jednak po raz kolejny zmieniła się 24 lutego 2022 roku.

Agresji Rosji na Ukrainę towarzyszył szereg działań destabilizujących ukraińską przestrzeń wirtualną. Hakerzy zaatakowali strony instytucji państwowych i finansowych, a portale informacyjne zaczęły być zalewane fake newsami. Ukraińcy stanęli do obrony, przedstawiciele organów państwowych zachęcali (nawet korzystając z oficjalnych kanałów komunikacyjnych) do kontrataków. W pomoc włączyli się polscy operatorzy, a członkowie Grupy MiŚOT przekazali serwery i inne urządzenia telekomunikacyjne dla kolegów z Ukrainy. Założono, że nieprzerwanie działająca łączność zwiększy szanse na odparcie napaści.

Dzięki obecności wielu podmiotów świadczących usługi dostępu do sieci oraz wsparciu płynącemu z Krzemowej Doliny łączność i możliwość kontaktu ze światem wydaje się w Ukrainie niezagrożona. Brak centralnego ośrodka będącego fundamentem krajowego internetu stał się kolejnym elementem zabezpieczenia tamtejszej infrastruktury krytycznej.

Innego zdania jest James Lewis, dyrektor programu technologii strategicznych w Centrum Studiów Strategicznych i Międzynarodowych w Waszyngtonie. Ekspert przekonuje, że Rosjanie, gdyby chcieli, to doprowadziliby do wyłączenia ukraińskiej sieci. Lewis uważa, iż najeźdźcy wykorzystują internet i sieć komórkową do śledzenia i podsłuchiwania Ukraińców. Z komunikatów przedstawianych przez Ukrainę wiemy jednak, że działa to również w drugą stronę.

Reperkusje cyberwojny dostrzegamy też w naszym kraju. Social media stały się przestrzenią, w której o zasięgi walczą trolle internetowe, by szerzyć rosyjską propagandę i fake newsy. To metoda mająca destabilizować sytuację w Polsce, gdyż obywatele rzucili się na pomoc uchodźcom. Szczucie na Ukraińców ma prowadzić do kolejnych podziałów w naszym kraju.

Sytuacja powinna skłonić polskich regulatorów do analizy krajobrazu sieciowego. Marcin Zemła, przedstawiciel projektu MdS (MiŚOT dla Security), jest zdania, że każdy dostawca internetu w Polsce powinien być uznany za operatora infrastruktury krytycznej. Byłby to ruch zwiększający nasze bezpieczeństwo zarówno w sieci, jak i w codziennym życiu.

Po zakończeniu działań zbrojnych Ukraina będzie dalej potrzebowała wsparcia krajów Zachodu. Już teraz mówi się, że konieczne będzie rozwiązanie zbliżone do tzw. planu Marshalla (inicjatywy Stanów Zjednoczonych mającej służyć odbudowie gospodarek krajów Europy Zachodniej po II wojnie światowej). Rekonstrukcja czeka też ukraińską infrastrukturę telekomunikacyjną. Jestem przekonany, że polscy operatorzy pomogą także wtedy. ■

DEZINFORMACJA ELEMENTEM CYBERWOJNY

KLAUDIA WOJCIECHOWSKA

Wojna w Ukrainie pokazała, że jesteśmy zdecydowanie w XXI wieku i działania militarne wkraczają też do świata cyfrowego. To pierwsza cyberwojna w historii ludzkości. Jednak w jej ramach odbywają się nie tylko cyberataki, mobilizacja hakerów i wycieki danych. To także walka za pomocą dezinformacji, do czego wykorzystywany jest internet i różne media społecznościowe. To w nich prezentowane są fake newsy i informacje propagandowe, które przygotowywane są przez ludzi związanych z Kremlem i rozprzestrzeniane przez prorosyjskich trolli.

Chociaż zarządzający platformami starają się z tym walczyć, to nie zawsze nadążają z reakcjami. Dlatego również użytkownicy powinni być czujni, sprawdzać informacje i nie przesyłać dalej postów, których nie zweryfikują. Ale żeby się do tego przygotować, warto wiedzieć, jak działa dezinformacja w trakcie tej wojny.

Twitter polem walki z dezinformacją

Twitter jest jedną z platform, które wykorzystywane są w wojnie dezinformacyjnej. Chociaż służy przekazywaniu informacji ze strony ukraińskiej, to także tam pojawiają się treści propagandowe z Rosji. Często załączane są do nich linki do materiałów przygotowanych i zamieszczanych przez źródła związane z Kremlem.

Walkę z dezinformacją prowadzi sam Twitter. Tnie on zasięgi wpisów, które zawierają linki do rosyjskich mediów państwowych, takich jak Sputnik czy RT. Już w ciągu pierwszych kilku dni od wybuchu wojny oznaczono kilkadziesiąt tysięcy takich wpisów i zmniejszono ich zasięg do 30 proc. Wprowadzono też zakaz reklamy na Twitterze dla serwisów wspierających rosyjską propagandę.

To nie wszystkie działania serwisu w tej walce. Oznaczono kilkadziesiąt tysięcy treści naruszających politykę w związku z manipulowaniem informacjami dotyczącymi ataku Rosji na Ukrainę. Zablokowano kilkadziesiąt tysięcy kont za działalność niezgodną ze standardami Twittera i spam. Ich cechą wspólną najczęściej było posługiwanie się hashtagiem #IStandWithPutin, który był popularny w skoordynowanej kampanii fałszywych kont. Ale dezinformacja nie zawsze ma tak łatwe do rozpoznania elementy. A serwis pomimo podejmowania kolejnych kroków w walce z dezinformacją czasem nie nadąża za rosyjskimi trollami i ich sposobami na umieszczanie takich treści oraz nakłanianie odbiorców do ich rozpowszechniania.

Cyberwojna na TikToku

Także na TikToku widoczna jest zmiana zachowań użytkowników i prezentowanych przez nich treści. Do daty wybuchu wojny w Ukrainie były to filmiki z tańcami, wyzwaniami, makijażami, pełne śmiechu i zabawy. Później platformę zdominowały instrukcje obsługi porzuconego czy zdobytego rosyjskiego sprzętu wojskowego, obrazy z atakowanych przez Rosję miast czy kadry uchodźców wojennych z drogi na Zachód. Influencerzy zaczęli wykorzystywać to medium do zachęcania ludzi na całym świecie do wsparcia Ukrainy.

Jednak pośród treści na TikToku nie brakuje też rosyjskiej propagandy. O skutecznym wykorzystaniu tego narzędzia przez Kreml informowała nawet Agencja Reutera. Pomieszanie informacji prawdziwych z propagandą utrudnia odróżnianie ich i sprawia, że odbiorcom coraz trudniej dotrzeć do rzetelnych informacji.

Żeby jeszcze bardziej zaciemnić obraz sytuacji i pozostawić szerzej otwartą furtkę dla rosyjskiej propagandy, rosyjski regulator mediów, internetu i telekomunikacji – Roskomnadzor zaczął apelować o ocenzurowanie TikToka. Pretekstem były treści brutalne w swojej wymowie, ale działania miały doprowadzić do próby zakneblowania strony ukraińskiej i niedopuszczenia do informowania przez nią świata o tym, co dzieje się w okupowanym przez Rosję kraju. Pozwoliłoby to nie tylko na przedstawienie rosyjskiej wersji całemu światu, ale też samym Rosjanom, którzy w kraju zarzucani są propagandą i którzy jedynie w mediach społecznościowych mogą poznać prawdę.

Jak walczyć z dezinformacją?

W podobny sposób jak na TikToku czy Twitterze dezinformacja pojawi się na Facebooku, Instagramie czy YouTubie. Trzeba z ostrożnością podchodzić do prezentowanych tam treści, by nie być trybikiem w machinie rosyjskiej propagandy rozprzestrzeniającej nieprawdziwe informacje. Często bywa to trudne, gdyż bazują one na silnych emocjach, więc można czasami udostępnić coś dalej pod ich wpływem, zanim jeszcze do głosu dojdzie rozum i zdążymy je zweryfikować.

Dlatego przede wszystkim należy stawiać na weryfikację. Nawet jeśli coś bardzo porusza, oburza, zasmuca, warto sprawdzić – najlepiej w kilku źródłach – czy dana wiadomość jest prawdziwa.

Istotne są też same konta, na których takie informacje się pojawiają. Rosyjskie trolle najczęściej posiadają konta z niewielką liczbą obserwujących lub zupełnie bez nich. Zakładane tylko na chwilę, by puścić w obieg fałszywą informację, mają też krótki termin funkcjonowania. To powinno zapalić lampkę ostrzegawczą w głowie odbiorcy.

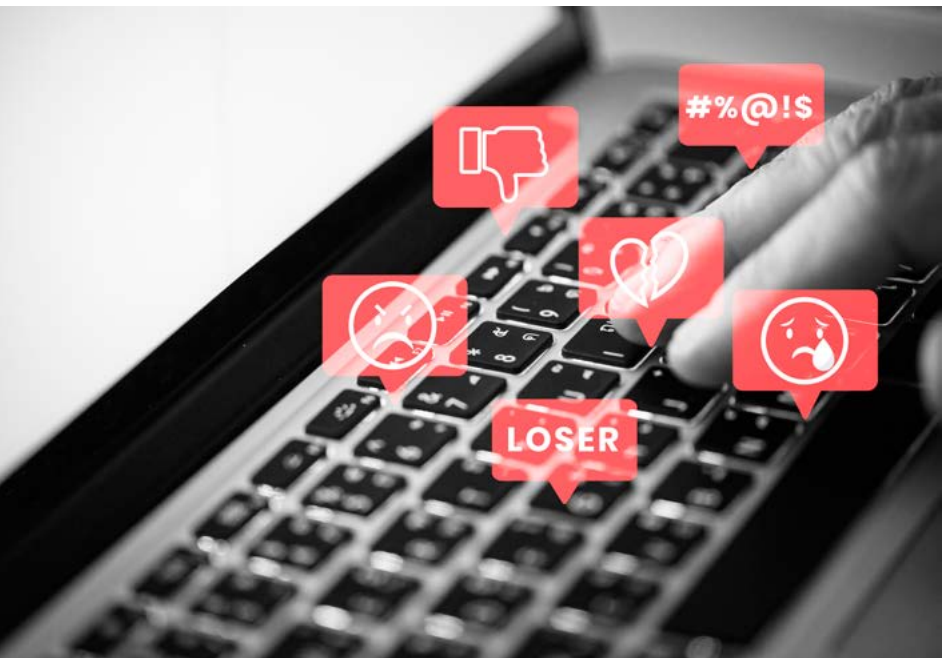
Warto być czujnym, bo bezrefleksyjne rozprzestrzenianie fałszywych informacji wspiera działania kremlowskiej propagandy, napędza panikę, powoduje nieracjonalne działania lub skłóca ze sobą ludzi. A tego nie potrzebujemy, obecnie jeszcze bardziej niż kiedykolwiek. ■

[źródła: cyberdefence24.pl, wirtualnemedia.pl]

HOLA, HOLA! NIE KARM TROLLA

MICHAŁ KOCH

Troll internetowy to osobnik napastliwy, irytujący i zwyczajnie chamski. Eksperci spodziewali się, że wraz z rozwojem kultury sieciowej zjawisko to zaniknie. Mylili się. Trolle internetowe nie wyginęły.



Sielanka w Horizon Worlds, cyfrowym świecie stworzonym przez Zuckerberga i firmę Meta, nie trwała długo. Jedna z użytkowniczek gry padła ofiarą molestowania. Cztery męskie awatary najpierw zaatakowały ją słownie, a później fizycznie. W Horizon Worlds gra się przy użyciu gogli rozszerzonej rzeczywistości Oculus, więc dla grającej doświadczenie było aż nazbyt realistyczne. Twórcy gry zareagowali błyskawicznie. Od tej pory każdego użytkownika chronić będzie specjalna strefa – Personal Boundary – będąca nieprzekraczalną granicą dla pozostałych towarzyszy zabawy.

Czy dawniej niestosowne zachowanie w sieci było zjawiskiem marginalnym? Odpowiedź nie jest jednoznaczna. Gracze zaadaptowali na swoje potrzeby zasady savoir-vivre'u, a osoby łamiące netykietę czekał ostracyzm. Społeczność sieciowa starała się trzymać poziom. Co się zatem zmieniło? Cóż, wraz z powszechnym dostępem do sieci pojawiło się też więcej osób, którym zależało przede wszystkim na zwróceniu na siebie uwagi. Krążący w Polsce w latach dwutysięcznych zwrot „dziecko Neo" (skrót od Neostrady, usługi Orange Polska) bywał określany jako początkowe stadium trolla internetowego. W grach MMORPG obecność trolli zależała od zaangażowania twórców. Niestosownego zachowania było mniej w pilnie moderowanym World of Warcraft, ale już w niezwykle popularnej w naszym kraju Tibii dość często padało się ofiarą słownego ataku.

Agresja i dyskryminacja nie są zachowaniami nowymi. Na przestrzeni wieków ludzkość doświadczyła ich wielokrotnie. Jako użytkownika internetu spotkało to i mnie. Począwszy od gier, aż po social media. Chociaż netykieta znalazła zwolenników, to wystarczy wejść do strefy komentarzy na jakimkolwiek portalu informacyjnym, aby doświadczyć przekleństw, fake newsów i werbalnej przemocy. Skala zjawiska jest tak duża, że spora część internautów odpuściła jakiekolwiek interakcje. Kilka polskich portali próbowało wdrożyć metody walki z hejtem i agresją m.in. poprzez weryfikowanie użytkowników lub po prostu wyłączenie możliwości komentowania artykułów. Bez efektów.

Omawiana sprawa jest też przedmiotem badań. Trollingiem zajmują się psychologowie, socjologowie, prawnicy, a także firmy technologiczne. Microsoft analizuje wirtualną przemoc od lat. Wyniki dotyczące kultury w sieci z 2021 roku są zastanawiające. W badaniu udział wzięło 11000 respondentów w dwóch grupach wiekowych 13–17 lat oraz 18–74. Ankietowani wyrazili swoje zdanie dotyczące zagrożeń internetowych, w tym nękania, trollingu i dyskryminacji.

Dla Polski wskaźnik kultury internautów wyniósł 65 proc., co oznacza poprawę o 4 proc. względem poprzedniego sondażu. Zatem internet u nas powinien być miejscem przyjaznym dla użytkownika. Jednak 41 proc. respondentów jest zdania, że zachowanie ludzi w sieci jest coraz gorsze.

Aż 56 proc. kobiet w sieci doświadcza niepożądanych interakcji. Skutkuje to zmniejszeniem zaufania w odniesieniu do osób poznanych w sieci, a także obniżeniem samooceny. 44 proc. użytkowników sieci z najmłodszego pokolenia wskazuje, że napotyka na niewłaściwe zachowania przy każdej okazji korzystania z internetu. Wzrost o 11 proc. jest niepokojący, gdyż dzieci surfujące online zaczynają traktować takie zachowania, jak coś naturalnego. Wirtualny świat sprawia, że zaczynamy mieć problemy w normalnej rzeczywistości.

Trolling to często ukryta agenda. Fińska dziennikarka Jessikka Aro, zajmująca się działaniem rosyjskiej propagandy, była miesiącami prześladowana i atakowana. Aro zebrała dowody popierające tezę, że brygady trolli, sterowane przez Kreml, sieją w cyberświecie dezinformację, fake newsy i hejt. Swoje doświadczenie przedstawiła w książce „Trolle Putina", w której umiejętnie opisuje, że współczesny świat – także sfera polityki – jest wielkim polem bitwy pomiędzy trollami internetowymi a cyberelfami – ochotnikami i działaczami społecznymi, których celem jest walka z prokremlowską propagandą. Wpływanie na wyniki wyborów za pomocą internautów to już smutny fakt. Problem, na który będziemy musieli szybko znaleźć remedium.

Większość z nas padła w sieci ofiarą ataku ze strony innego internauty. Budując nową wirtualną przestrzeń (tzw. Web 3.0), musimy rozwiązać problem trolli. Na szczęście zjawisko jest coraz częściej piętnowane. Według badania Microsoft sami internauci dostrzegają potrzebę walki z trollingiem. Wśród dostępnych możliwości jest wprowadzenie lepszej edukacji (także cyfrowej), ostrzejszej moderacji i innowacyjnych sposobów na weryfikowanie tożsamości komentującego.

Jedną z zalet internetu jest anonimowość. Niestety jest to również jedna z największych jego wad. ■

SZYBKOŚĆ PRZEKAZYWANIA DANYCH POLICJI MA ZNACZENIE

MAREK NOWAK

Operator publicznej sieci telekomunikacyjnej, a także dostawca publicznie dostępnych usług telekomunikacyjnych, są ustawowo zobowiązani zatrzymywać i przechowywać szereg danych, które są przez nich generowane lub przetwarzane. Ma to ułatwić ściganie przestępstw.

Artykuł 180c ustawy Prawo telekomunikacyjne wskazuje, że archiwizowane powinny być dane niezbędne do:

- ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego inicjującego połączenie oraz tego, do którego kierowane jest połączenie,
- określenia: daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia, lokalizacji telekomunikacyjnego urządzenia końcowego.

Obowiązek przechowywania danych jest ograniczony terytorialnie (granicami Rzeczypospolitej Polskiej) oraz czasowo (obejmuje okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia). Szczególnie ograniczenie czasowe może mieć duże znaczenie w praktyce ścigania przestępstw.

Dowód w sprawie

– Obowiązek, o którym mowa, ma w praktyce pozwolić organom ścigania wykrywać i oskarżać sprawców przestępstw popełnianych za pomocą środków porozumiewania się na odległość – mówi Marcin Zemła ze spółki Informatics z Jaworzna, współpracującej przy projekcie MiŚOT dla Security. – Wskazanie adresu IP lub numeru telefonu bywa bardzo ważnym, a nawet kluczowym, środkiem dowodowym w wielu postępowaniach.

Operatorzy przechowują więc dane (na własny koszt) i w razie potrzeby udostępniają je na żądanie policji, Agencji Bezpieczeństwa Wewnętrznego, Centralnego Biura Antykorupcyjnego, Centralnego Biura Śledczego, a także sądu i prokuratury, na zasadach i w trybie określonym w przepisach. Zobowiązani są również chronić je przed przypadkowym lub bezprawnym zniszczeniem, a także utratą lub zmianą, nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem.

Procedury

– Choć operatorzy dotrzymują wszystkich obowiązków i procedur, problemem postępowań prowadzonych przez organy ścigania bywa ich przewlekłość – podkreśla Marcin Zemła. – Z drugiej zaś strony z upływem roku operator zobowiązany jest dane zniszczyć, o ile nie zostały uprzednio formalnie zabezpieczone na żądanie odpowiednich służb.

W efekcie trwa więc wyścig z czasem, w którym sukces zależy także od dobrej woli i sprawności działania operatorów.

– W praktyce, gdy policja zabezpiecza sprzęt komputerowy, przekazuje go następnie do laboratorium Komendy Wojewódzkiej, gdzie informatyk śledczy prowadzi analizy trwające nawet kilka miesięcy – wyjaśnia Marcin Zemła. – Wtedy też okazuje się, że doszło do połączenia związanego z przestępstwem i konieczne jest ustalenie danych klienta końcowego posługującego się (w określonym momencie) określonym IP, po czym kierowane jest pismo do operatora.

Choć procedury policyjne nie wymagają od dostawców publicznie dostępnych usług telekomunikacyjnych niezwłocznego działania, warto pamiętać, że w tym momencie tempo postępowania, kolejne podejmowane przez policję kroki, a co za tym idzie czyjeś bezpieczeństwo, zależy właśnie od szybkiej reakcji ISP. ■

ŚWIADCZENIE USŁUG BSA JAKO SZANSA NA OPTYMALIZACJĘ PROCESÓW

Ile można zyskać i jak zoptymalizować procesy od strony prawnej oraz organizacyjnej?

MARTA HERÓD, RADCA PRAWNY W KANCELARII PRAWNEJ BRIGHTSPOT

Niezależnie od tego, czy udostępniają Państwo czy korzystają Państwo z usług międzyoperatorskich, każdy z procesów dostępu powinien być przemyślany pod względem biznesowym. Świadczenie usług hurtowych może nie być jedną z wiodących „nóg" biznesu telekomunikacyjnego dla ISP, ale ten, kto prawidłowo wdrożył takie usługi w swojej sieci, potwierdza szereg korzyści, jakie z tego płyną (i nie chodzi nam tu tylko o fakturę za zrealizowane usługi).

W tym artykule pokażemy Państwu, że przy prawidłowej organizacji pracy techników, ustandaryzowaniu procesów komunikacji z kontrahentem oraz zastosowaniu pewnych zabezpieczeń w umowach między operatorskich BSA świadczenie usług BSA przynosi znaczące korzyści finansowe oraz wizerunkowe. Ponadto spojrzymy na BSA z perspektywy operatora udostępniającego – czyli operatora, który udostępnia własną sieć dla celu podłączenia, w tzw. ostatniej linii, abonentów innego operatora.

Proces świadczenia usług BSA może wydawać się skomplikowany i czasochłonny, ale my postaramy się udowodnić Państwu, że przy niskim wkładzie wejścia w ten proces można wiele zyskać.

1. Większość ISP ma służby techniczne odpowiednie dla świadczenia BSA

Wielu operatorów podpisujących umowy BSA zastanawia się, czy jego służby techniczne i BOK podołają nowemu zadaniu. Często myśli się o zatrudnianiu dodatkowych osób, rozważa się dodatkowe szkolenia – to wszystko generuje jednak dodatkowe koszty i w efekcie ISP rezygnuje z tego przedsięwzięcia. Wielu operatorów chcących skorzystać z usług BSA obawia się bowiem przede wszystkim skali czynności, które należy wykonać w związku z podjęciem współpracy w zakresie świadczenia usług BSA. Obawy te pogłębiane są przez kolejne zapisy z umów dotyczące m.in. kar umownych za niespełnianie terminów instalacji, uszkodzeń czy powtórzeń oraz przez inne postanowienia umowne, które mogą stanowić mechanizm obniżenia opłat za świadczenie usług BSA – co w konsekwencji będzie doprowadzało do uszczuplenia wynagrodzenia na fakturze rozliczającej usługę. Postanowienia te mogą budzić duży niepokój, w tym mogą nawet skutecznie zniechęcić do podjęcia się współpracy na zasadach BSA.

Operator musi rozważyć, czy kompetencje jego pracowników są na tyle wysokie i czy posiada on zasoby w odpowiedniej ilości.

Pytanie więc brzmi: czy damy radę?

Odpowiedź brzmi: TAK.

Z naszego doświadczenia i obserwacji wynika, że dziś ci operatorzy, którzy podpisali umowy BSA, nie tylko wysycają sieci końcówkami z migracji klientów, ale również osiągają lepsze wyniki w zakresie efektywności swoich pracowników. Okazuje się, że przy zapewnieniu stałych dostaw zamówień, zastosowaniu sztywnych terminów realizacji zamówień na usługę i pilnowaniu wdrożonych wskaźników monterzy potrafią pracować na bardzo wysokim poziomie efektywności i jakości, co bezpośrednio przekłada się na lepsze wyniki finansowe, jak również możliwość zaproponowania większej stawki wynagrodzenia ekipie technicznej. Transakcja ta jest zatem korzystna dla obu stron – w czasach inflacji pracownicy mogą liczyć na podwyżki, a w zamian możliwe jest zbudowanie zespołu pracowników o większych kompetencjach i lepszej efektywności.

2. Moja ekipa a model umowy BSA – co wybrać?

Istotne jest dokładne przeanalizowanie warunków świadczenia usług BSA przed podpisaniem samej umowy. Nie bez znaczenia jest właśnie to, czy BSA ma być świadczone w tzw. modelu jedno- czy dwuekipowym, a więc czy obok umowy BSA powinna być zawarta umowa o partnerstwo techniczne czy też nie. Decyzja co do stosowanego modelu powinna być wcześniej przeanalizowana między innymi pod kątem tego, kto wykonuje instalacje, kto zapewnia sprzęt ONT oraz co ze zwrotami sprzętu i utrzymywaniem stanów magazynowych. Późniejsze negocjowanie warunków umów BSA powinno być dostosowane szczególnie do realiów, w jakich świadczenie usług BSA będzie technicznie wykonalne i opłacalne.

Istotne jest przy tym dokładne opisanie w umowie zasad uruchomienia usług – tj. przyjmowania zamówień, godzin ich przyjmowania oraz wskazania okresu czasowego i ilościowego ich obsługi. Skoro bowiem Państwa ekipa monterów, obok instalacji i aktywacji klientów własnych, ma obsługiwać także uruchomienia usług dla hurtu, to ich czas pracy powinien zostać dostosowany i usystematyzowany do obsługi hurtu. Nie bez znaczenia pozostaje jasne określenie zasad anulacji zamówień z powodów niezależnych od obu operatorów współpracujących, a które to zapisy powinny jasno określać zasady rozliczeń w razie dokonania takiej anulacji. Niejednokrotnie bowiem spotykamy się z zapisami, które są niedostosowane do realiów, jeżeli chodzi o obsługę usługi od strony klienta końcowego – który często zmienia zdanie albo rezygnuje z usługi w ostatniej chwili. Operator udostępniający nie powinien być przy tym stratny, bo był gotowy do uruchomienia usługi, a operator korzystający może nie mieć wystarczającego wpływu na zatrzymanie klienta. Te wszystkie nieścisłości w umowach można wyeliminować w trakcie ich negocjacji przez wykwalifikowany w tym zakresie zespół.

3. Czy zatem ISP musi zatrudnić dodatkowe osoby, aby prawidłowo obsłużyć usługę BSA?

Z naszego doświadczenia wynika, że standardowy ISP nie musi zwiększać zespołu, aby wdrożyć usługi BSA w swojej sieci. Oczywiście wszystko zależy od aktualnej struktury organizacyjnej firmy i poziomie efektywności, ale zwykle nie ma potrzeby rekrutacji dodatkowych ekip, dyspozytorów czy koordynatorów na stałe do obsługi kontraktów BSA oraz umów o partnerstwo techniczne.

Przy przygotowaniu niniejszego artykułu, w ramach anegdoty, Paweł przytoczył sytuację u jednego z operatorów: „Koniec roku, czas inwentaryzacji. Okazuje się, że jak zwykle brakuje kilku modemów i routerów z instalacji własnych. Kilkaset instalacji w ciągu roku – zdarza się. Obok podsumowanie inwentaryzacji z modemów operatora korzystającego z usługi BSA. Instalacji dwa razy więcej niż instalacji własnych. Ilość zgubionego sprzętu? Zero."

Jaki wniosek? Przy odpowiednim zmotywowaniu ludzi i dobrym nadzorze oraz wsparciu pracownicy potrafią bardzo dobrze pracować i pilnować narzędzi oraz materiałów potrzebnych do swojej pracy. Co za tym idzie, terminowo i prawidłowo wykonane zlecenia nie będą pociągać za sobą konieczności zapłaty kar umownych, a nawet jeśli zdarzą się pojedyncze „wpadki", to w dobrze wypracowanych umowach nie powinny one mieć wpływu na wysokość wynagrodzenia czy aktualizację obowiązku zapłaty bonifikat na rzecz drugiej strony.

Podsumowując, ci, którzy świadczą usługi BSA, dziś mogą pochwalić się dużą ilością nowych końcówek w sieci i wyższym poziomem organizacji, efektywności i jakości. Współpraca międzyoperatorska, często z dużym operatorem, uczy wielu nowych i dobrych nawyków, a ekipa techników szybko się do odpowiedniego rytmu dostosuje. Dobre nawyki wyrobione w trakcie obsługi hurtu mogą być wykorzystane do własnych potrzeb. Ponadto dobrze skoordynowana współpraca międzyoperatorska może mieć wpływ na wizerunek przedsiębiorstwa ISP jako rzetelnego kontrahenta.

Oczywiście obok zapisów umownych mających zoptymalizować koszty obsługi od strony technicznej warto także przyjrzeć się dokładnie innym zapisom umownym BSA – począwszy od składanych oświadczeń o braku obciążenia sieci (a przecież często brane pożyczki są zabezpieczone zastawem rejestrowym, co przy proponowanych sztywnych zapisach uniemożliwiałoby zawarcie umowy BSA), przechodząc przez zapisy dotyczące wpływu potencjalnych transakcji sprzedaży sieci, na której usługi BSA są świadczone, zachowania integralności sieci i jej bezpieczeństwa czy migracji abonentów, a kończąc na zapisach dotyczących zabezpieczeń w razie niewykonywania umowy przez operatora udostępniającego oraz operatora korzystającego.

Uważamy jednak, że w negocjowaniu umów BSA warto skupić się na zapisach dotyczących właśnie obsługi umowy od strony wykonawczej – od tych zapisów może bowiem zależeć sukces wdrożenia usługi BSA. ■

WSPÓŁAUTORZY TEKSTU:

Paweł Licznar

Doradza w zakresie realizacji umów rBSA, wdrażania wskaźników efektywności i współpracy międzyoperatorskiej. Partner technologiczny grupy Brightspot Law and Consulting. Były dyrektor jednej ze stref utrzymaniowych Orange Polska.

Marta Heród

Radca prawny w Kancelarii Radcy Prawnego Katarzyny Orzeł wchodzącej w skład grupy Brightspot Law and Consulting. Doradza ISP w procesie negocjowania i zawierania umów rBSA oraz BSA, a także w przygotowaniu pakietu dokumentów dla potrzeb rozpoczęcia świadczenia usług BSA.

NAJNOWSZA PORCJA WIEDZY MiŚOT AKADEMII

MARCIN OROCZ

Spotkania mogą być emocjonalnym rollercoasterem, zwłaszcza jeśli występują na nich decydenci, a nastroje są napięte. Komentarz lub sugestia ze strony członka zespołu może wywołać silną reakcję, w tym frustrację, niepewność co do swojego stanowiska lub złość. Wyzwanie polega na tym, aby zachować na tyle opanowania, by móc jasno myśleć i skutecznie się komunikować. Unikaj przesadnych reakcji, które mogą pozostać w pamięci innych osób i wymazać wiele pozytywnych osiągnięć.

Gdy zrobi się gorąco, możesz podejmować decyzje dotyczące zarządzania samym sobą. O technikach opanowania podczas spotkań pisze na stronie akademia.misot.pl Adrianna Wardzała, ekspert od komunikacji w MiŚOT Akademii.

IPv6

Dla większości internautów fakt, czy używają IPv4 czy IPv6, jest bez znaczenia – podczas codziennego korzystania z sieci nie będą dostrzegać różnicy. Nie oznacza to jednak, że te protokoły są identyczne i że można je dowolnie między sobą wymieniać. Słyszymy, że IPv4 ma zostać zastąpione przez IPv6, ale jakie są różnice między tym protokołami? Kurs dotyczący IPv6 przygotowany przez naszych branżowych ekspertów to materiały multimedialne, dodatkowe materiały poszerzające wiedzę techniczną i możliwość zdobycia certyfikatu MiŚOT Akademii po pozytywnym zaliczeniu testu.

Metoda prezentowania oferty w pięciu krokach

Jeśli jesteś handlowcem lub menedżerem, który odpowiada za sprzedaż, i planujesz cykliczne spotkania ze swoimi klientami i kontrahentami – to szkolenie jest dla ciebie! Na szkoleniu zaprezentuję ci metodę przygotowania się do wizyty z klientem w sposób, który zwiększy jej efektywność, a także sprawi, że twoja wizyta handlowa stanie się skuteczniejsza. Szkolenie w formie multimedialnej (szkolenie video) prowadzi praktyk sprzedaży Zbigniew Żuk. Jest ono skierowane przede wszystkim do operatorów współpracujących w obszarze B2B, tworzących oferty handlowe i budujących długotrwałą współpracę z firmami, instytucjami czy przedsiębiorcami. Metoda pięciu kroków sprawdzi się również w tworzeniu nowej koncepcji oferty dla klienta indywidualnego.

Wyzwania branży w obszarze sprzedaży

Podczas wizyt w terenie czy obserwacji pracy biur obsługi klienta można coraz częściej zauważyć brak efektywności handlowców. Do tego dochodzi duża rotacja wśród nowych pracowników, małe budżety na edukację i podnoszenie kompetencji oraz brak współpracy między sprzedażą a innymi działami.

Najważniejszym celem szkoleń dla handlowców jest zwiększenie sprzedaży firmy. Często jednak schodzi on na dalszy plan na rzecz innych: integracji (udanej imprezy) i dbania o dobre samopoczucie handlowców. Jasne, takie inicjatywy są ważne, ale bez realizacji celu nadrzędnego szkolenie nie przełoży się na wyniki finansowe firmy, na które finalnie zwracamy uwagę.

Okazuje się, że nigdy nie ma dobrego momentu na szkolenia. Zadaniem szkoleń dla handlowców jest to, aby ludzie pracujący w sprzedaży byli przygotowani na zawirowania rynkowe. Powinniście zatem zawsze szkolić pracowników jeszcze zanim rynek zwolni, zanim wam siądzie sprzedaż. Gdy to już nastąpi, będzie za późno. Stracicie tygodnie lub miesiące, do czasu aż handlowcy odbudują sprzedaż. Dlatego warto się szkolić zarówno w dobrych, jak i przeciętnych okresach.

Jeśli nie chcecie odrywać handlowców od pracy (bo macie żniwa), to MiŚOT Akademia jest najlepszym do tego miejscem, udostępniającym szkolenia w wersji online – kilka minut dziennie, małymi dawkami, ale regularnie przez kilka miesięcy. Dzięki takiemu podejściu firma nie straci sprzedaży, a handlowcy przez cały czas będą mogli zdobywać nowe umiejętności.

Pandemia pokazała, że nie trzeba organizować szkoleń „jak wesela", czyli w formie dwudniowego projektu, z potężnym budżetem na hotele, sale, noclegi, imprezę wieczorną i integrację w terenie. Okazuje się, że to, co przed pandemią wydawało się być nie do przyjęcia, dziś się sprawdza. Możecie więc zamiast jednego szkolenia w ciągu roku (które skonsumuje cały budżet szkoleniowy) zorganizować wiele krótszych sesji (webinarowych, po 2-3 godziny) lub umówić się z trenerem na cztery jedniowe spotkania w ciągu roku i uzupełnić ten proces profesjonalnymi, nowoczesnymi szkoleniami, dzięki którym pracownicy mogą się uczyć raptem 10 minut dziennie. Możecie też dać im dostęp do 40-50 krótkich wideo sesji szkoleniowych (po 5-10 minut) i uzupełnić je jedną sesją szkoleniową na sali.

„To w interesie właścicieli leży, aby szkolenie było skuteczne (a mniej „fajne"). Trzeba zacząć mierzyć, czy ludzie czegokolwiek się nauczyli, a nie tylko pytać o ich ocenę. Z drugiej strony władze firmy są często „ponad to" – dla nich szkolenie sił sprzedaży to drobiazg, którym nie chcą się zajmować, bo są od ważniejszych spraw. Każdy udaje, sprzedaż nie rośnie, a pieniądze są źle wydawane" – pisze w raporcie „19 powodów, dlaczego szkolenia dla handlowców nie działają" Przemysław Mik, prezes SalesOn – dostawcy platformy szkoleniowej MiŚOT Akademii. ■

Na hasło „ictprofessional" dostaniecie 15% rabatu na pakiety szkoleniowe MiŚOT Akademii na sklep.misot.pl (wymagany EPID).

sklep.misot.pl

akademia.misot.pl

TERMINOLOGIA KONSOLIDACYJNA: GRUPA KAPITAŁOWA

KRZYSZTOF ZAWADZKI

Podejmując próbę wyrównania stanu wiedzy w zakresie terminologii konsolidacyjnej, rozpoczynamy przedstawianie pojęć, które są lub mogą być wykorzystywane do opisu poczynań i zamierzeń związanych z budową Grupy MiŚOT.

Dobre zrozumienie jest podstawą każdej debaty i stanowi kluczowy czynnik sukcesu w osiągnięciu kompromisu i zawarciu porozumienia. Bez dobrego zrozumienia nie mam mowy o przekonaniu szerszej grupy beneficjentów, jakie korzyści osiągną z danego projektu, a co więcej, pojawia się ryzyko rozczarowania, gdy każdy z nich w odmienny sposób będzie rozumiał swoje oczekiwania. Jak często zdarza się nam w toku zażartej dyskusji dojść do konkluzji – ale czy oby na pewno mówimy o tym samym? No właśnie! Właściwa komunikacja jest bardzo ważna, gdyż jest narzędziem do rozwiązywania i unikania konfliktów, a jej efektem końcowym jest konsensus między rozmawiającymi osobami.

Gdy „ojcowie założyciele" Grupy mówią: „naszym celem było zbudowanie stabilnej i wiarygodnej na rynku Grupy MiŚOT", mają na myśli utworzenie grupy powiązanych ze sobą spółek, które wszystkie razem będą działały na rzecz MiŚOT-ów, realizując wspólną strategię i nie konkurując ani między sobą, ani też z MiŚOT-ami. Przejdźmy więc do zdefiniowania, czym jest grupa kapitałowa. Warto tutaj przytoczyć kilka cech ją charakteryzujących:

- grupy kapitałowe są zjawiskiem biznesowym powszechnie występującym praktycznie we wszystkich państwach na całym świecie, w których działają mechanizmy gospodarki rynkowej;
- grupy kapitałowe są tworzone, aby rozwijać działalność gospodarczą, sprostać wyzwaniom konkurencji i rynku w myśl zasady „w grupie łatwiej, bezpieczniej i silniej";
- grupy kapitałowe nie są tworami przypadkowymi, ale organizmami celowymi, logicznie powiązanymi i wzajemnie uzależnionymi (późniejsze wypadnięcie jednego ogniwa często powoduje efekt domina), a ich powstanie poprzedzają szczegółowe analizy i symulacje produkcyjne oraz finansowe;
- w grupie kapitałowej występuje zjawisko wspólnoty interesów, które jest cechą

wyróżniającą takie ugrupowanie gospodarcze, a wszelkie działania podejmowane w ramach grupy kapitałowej powinny mieć swoje uzasadnienie we wspólnym interesie grupy;

- grupy kapitałowa nie ma odrębnej osobowości prawnej, a wspólny interes niekoniecznie polega na dążeniu do dystrybucji zysków. Wspólny interes grupy polega na dywersyfikacji aktywności biznesowej w celu uniknięcia negatywnych konsekwencji związanych z niekorzystnym odwróceniem koniunktury rynkowej, wprowadzaniu niezbędnych reform w strukturze organizacyjnej, wejściu na nowe rynki, polepszeniu zarządzania;
- wspólny interes grupy polega na realizacji interesu ekonomicznego i finansowego. Przez interes ekonomiczny należy rozumieć zwiększenie efektywności zarządzania, rozłożenie ryzyka prowadzonej działalności, tworzenie elastycznej struktury organizacyjnej, osiąganie efektów synergii, prawnie dozwoloną optymalizację podatkową, ekspansję rynkową, zwiększanie wiarygodności poszczególnych spółek z grupy. Interes finansowy polega na osiąganiu korzyści z tytułu wspólnego zarządzania finansami grupy kapitałowej (np. odsetki, dostęp do linii kredytowej, gwarancje bankowe, zarządzanie płynnością grupy itp.);
- grupa kapitałowa jest w swej istocie źródłem szans i minimalizacji ryzyka rynkowego;
- celem członków grupy kapitałowej powinna być koncentracja na podejmowaniu działań ukierunkowanych na realizację interesu (wspólnego) grupy kapitałowej z uwzględnieniem uzasadnionych interesów wierzycieli i wspólników mniejszościowych;
- podejmowanie decyzji ze skutkiem dla grupy kapitałowej oraz współpraca w ramach grupy powinny opierać się na wyważeniu interesów interesariuszy grupy kapitałowej, w szczególności MiŚOT-ów.

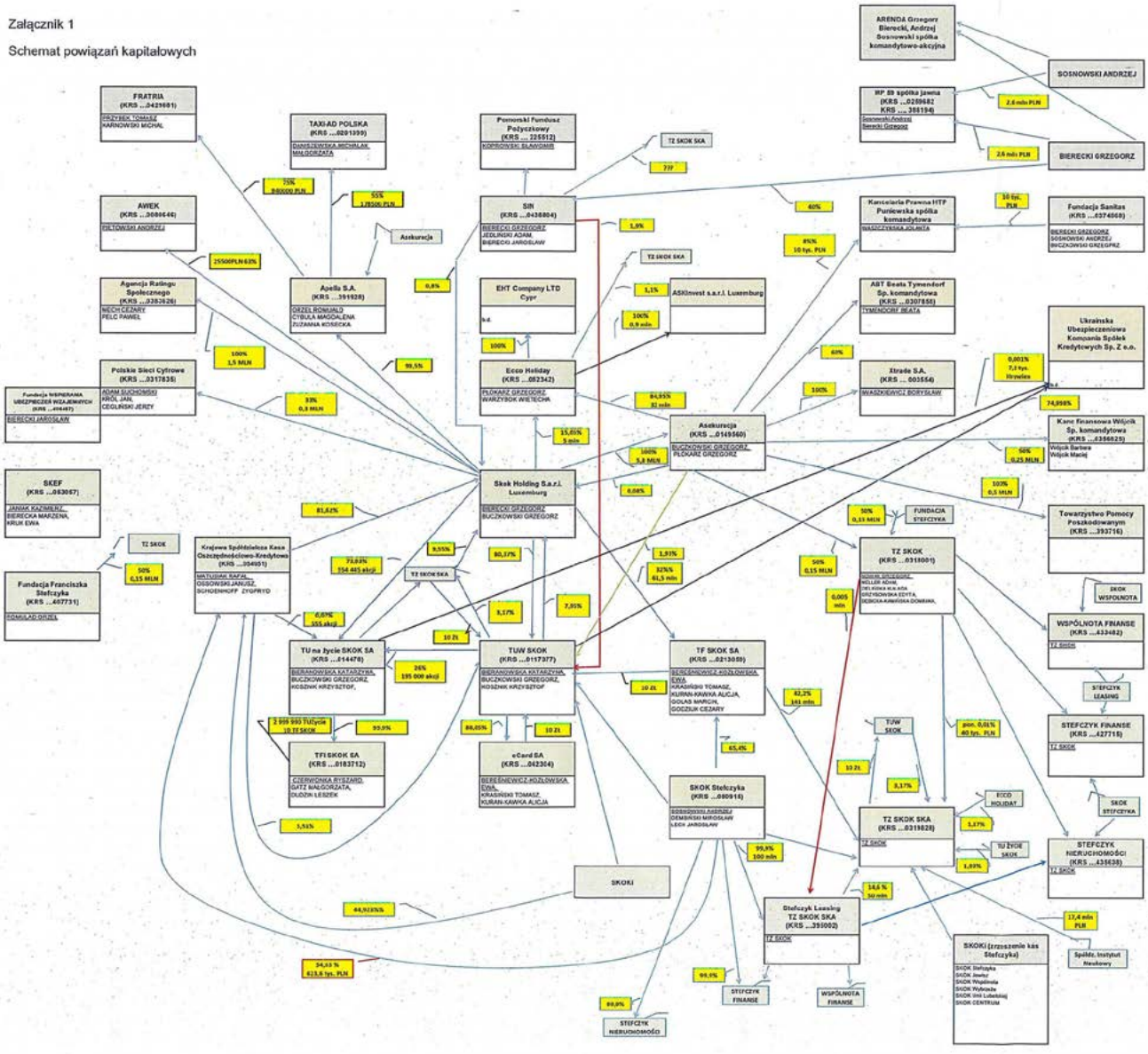
Wszystkie wymienione cechy grupy kapitałowej są niewątpliwie jej dobrą „stroną mocy". Jest jednak i ciemna strona, która służy zaciemnieniu obrazu przepływu kapitałów i źródła pochodzenia kapitału, zidentyfikowaniu beneficjentów rzeczywistych (właściwych osób sprawujących kontrolę) czy nawet unikaniu opodatkowania. Zbyt duża i nieuzasadniona ilość podmiotów w grupie kapitałowej oraz ich wzajemnych powiązań może zdecydowanie utrudniać zrozumienie modelu biznesowego panującego w grupie kapitałowej, rzeczywistego celu jej powołania oraz, co gorsze, powodować powstawanie rzeczywistego konfliktu interesów w grupie kapitałowej.

Przykładem bardzo rozbudowanej i bardzo trudnej do zrozumienia grupy kapitałowej może być grupa SKOK, która była przedmiotem kontroli Komisji Nadzoru Finansowego w 2014 r.

Grupa MiŚOT tworzona jest w sposób transparentny i poznając jej strukturę, łatwo przeanalizować przepływ kapitału i źródła jego pochodzenia i beneficjentów, którymi są oczywiście tworzący ją operatorzy.

Załącznik 1

Schemat powiązań kapitałowych



Źródło: https://biznes.trojmiasto.pl/Raport-KNF-na-temat-powiazan-kapitalowych-i-personalnych-w-SKOK-n84595.html

Kto kontroluje grupę kapitałową?

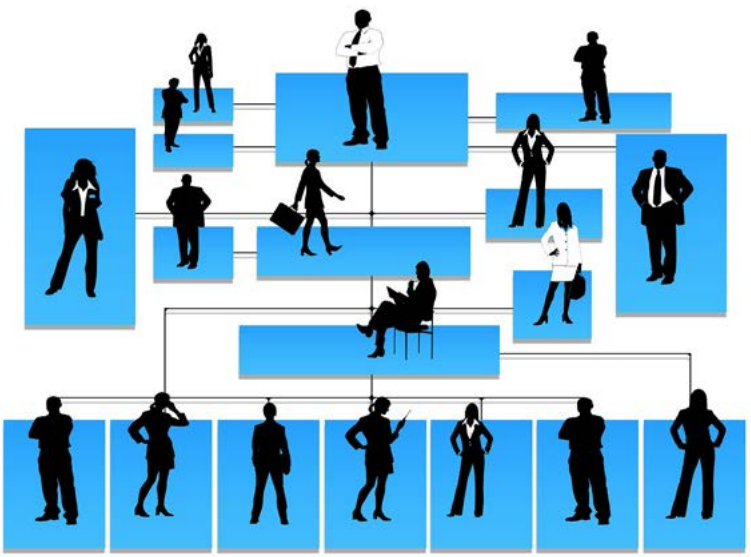
W Polsce obowiązują dwojakiego rodzaju regulacje w rachunkowości dotyczące zakresu kontroli. Pierwsze są bardziej ogólne i powszechniej stosowane przez przedsiębiorstwa takie jak MiŚOT-y, drugie zaś zdecydowanie bardziej rozbudowane i szczegółowe, stosowane przez emitentów papierów wartościowych notowanych na rynku regulowanym. Celowo nie poruszam w tym krótkim artykule kwestii prawa handlowego z uwagi na jego rozległość i wielowątkowość.

Ogólnie i szczególnie

Ustawa o rachunkowości, jako zdecydowanie bardziej powszechnie stosowana regulacja, definiuje kontrolę w sposób ogólny, jako zdolność jednego podmiotu do kierowania polityką finansową i operacyjną innego podmiotu, w celu osiągania korzyści ekonomicznych z jej działalności. Innymi słowy, jeżeli jeden podmiot poprzez posiadaną odpowiednią ilość głosów w kapitale zakładowym (najczęściej stanowiących więcej niż 50%) może przegłosować kluczowe decyzje w spółce, w tym te dotyczące powoływania jej organów, to bez wątpienia mamy do czynienia ze zdolnością do kierowania jej polityką.

Drugie regulacje brzmiące bardziej globalnie i mające międzynarodowy charakter to Międzynarodowe Standardy Sprawozdawczości Finansowej (MSSF). Zapisy tej regulacji są bardziej zawiłe i skomplikowane. Z grubsza zaś wskazują, że kontrola występuje nie tylko w przypadku, gdy jeden podmiot (zwany inwestorem) posiada władzę nad drugim podmiotem, którego udziały lub akcje nabył. Oznacza to, że kontrola może być sprawowana w różny sposób, niekoniecznie tylko w drodze posiadania więcej niż 50 proc. praw głosu. Jeżeli taki inwestor dysponuje jakimikolwiek prawami dającymi mu możliwość bieżącego kierowania działaniami, które znacząco wpływają na wyniki finansowe tej jednostki, to pomimo posiadania mniej niż 50 proc. głosów w kapitale również sprawuje on kontrolę. Niestety w wielu przypadkach ocena sprawowania władzy wynikająca z ustaleń umownych jest bardzo złożona i wymaga rozważenia więcej niż jednego czynnika. Przykładem takich praw może być np. prawo do powoływania i wynagradzania kluczowego personelu kierowniczego jednostki, w której dokonano inwestycji lub dostawców usług oraz rozwiązywania z nimi umów o świadczenie usług bądź umów o pracę.

Jednym z podstawowych warunków zapewniających skuteczną kontrolę jest obecność w grupie kapitałowej sprawnych mechanizmów nadzoru korporacyjnego i/lub nadzoru właścicielskiego. Należy w tym miejscu zwrócić uwagę na pewne różnice, które istnieją pomiędzy nadzorem właścicielskim a nadzorem korporacyjnym, które to pojęcia bardzo często są ze sobą utożsamiane lub używane zamiennie. Nadzór właścicielski jest z pewnością pojęciem węższym od nadzoru korporacyjnego, obejmując jedynie zagadnienia związane z prawami akcjonariuszy do ich majątku powierzonego kadrze, która zarządza przedsiębiorstwem. Pojęcie nadzoru korporacyjnego zaś ma szersze znaczenie i swoim zasięgiem obejmuje formalną i nieformalną strukturę wpływów na najważniejsze decyzje podejmowane przez menedżerów. Dotyczy ono nie tylko właścicieli kapitału, ale wszystkich grup interesów (interesariuszy) zainteresowanych sytuacją przedsiębiorstwa, takich, na które sposób funkcjonowania przedsiębiorstwa ma wpływ (pracownicy, związki zawodowe, dostawcy, odbiorcy, kooperanci). Powodami, które spowodowały rozszerzenie zakresu nadzoru właścicielskiego na szerzej rozumiany nadzór korporacyjny, były:



Źródło grafiki: ceo.com.pl

„Gdy „ojcowie założyciele" Grupy mówią: „naszym celem było zbudowanie stabilnej i wiarygodnej na rynku Grupy MiŚOT", mają na myśli utworzenie grupy powiązanych ze sobą spółek, które wszystkie razem będą działały na rzecz MiŚOT-ów, realizując wspólną strategię i nie konkurując ani między sobą, ani też z MiŚOT-ami.

- pogłębiające się procesy globalizacji, które wpłynęły na zmiany w otoczeniu organizacji;
- nasilająca się konkurencja, która zmusza do poszukiwania bardziej skutecznych, efektywnych rozwiązań umożliwiających pełne wykorzystanie posiadanych zasobów i rozwój.

Warto zwrócić uwagę, że nadzór właścicielski nie jest pojęciem zdefiniowanym w przepisach prawa. Nadzór korporacyjny wiąże się z istnieniem sieci relacji między kadrą zarządzającą spółek, ich organami zarządzająco-nadzorczymi, wspólnikami/akcjonariuszami i innymi interesariuszami (podmiotami zainteresowanymi działaniem spółki). Nadzór korporacyjny oferuje ponadto strukturę, za pośrednictwem której ustalane są cele spółki, środki realizacji tych celów oraz środki umożliwiające śledzenie wyników spółki. Dobry nadzór korporacyjny powinien w sposób właściwy stymulować organy spółki i kadrę zarządzającą do osiągania celów, których realizacja leży w interesie spółki i jej wspólników/akcjonariuszy, a także powinien ułatwiać skuteczne śledzenie wyników, sprzyjające tym samym bardziej efektywnemu wykorzystaniu zasobów przez firmy. Funkcjonowanie skutecznego systemu nadzoru korporacyjnego, czy to w poszczególnych spółkach, czy też w całej gospodarce, przyczynia się do uzyskania większego zaufania, które jest istotnym czynnikiem zapewniającym sprawne działanie gospodarki rynkowej.

Biorąc pod uwagę wskazane definicje, nadzór właścicielski można więc określić jako sposób egzekwowania praw własnościowych, w relacji pomiędzy akcjonariuszami, ich formalnymi przedstawicielami a zarządem, sprawowany przez właściciela kapitału lub grupę właścicieli. ■

DUŻE ZMIANY NA POLSKIM RYNKU PALIW I ENERGII

EMIL RÓŻAŃSKI

Agresja Rosji na Ukrainę przyspieszy zmiany w polskiej energetyce oraz na rynkach gazu i ropy. Ceny raczej nie spadną, ale zmieniamy Rosję na innych dostawców węgla, gazu i ropy.

Wojna na Ukrainie przełożyła się na rynek energii i surowców energetycznych w Unii Europejskiej, w tym Polsce. Było to widać po cenach energii i gazu na polskiej Towarowej Giełdzie Energii (TGE). W marcu 2022 r. średnia cena na Rynku Dnia Następnego (RDN), czyli rynku spot, na TGE ukształtowała się na poziomie 683,59 zł za MWh i jest to wzrost aż o 157,70 zł na MWh w porównaniu do lutego.

Droższy gaz i energia na giełdzie

Na rynku terminowym średnia cena kontraktu rocznego z tzw. dostawą pasmową w roku 2023 wyniosła w marcu 2022 r. 714,64 zł za MWh, co stanowi wzrost o 96,34 zł na MWh względem analogicznej ceny tego kontraktu w lutym 2022 r.

Podobnie było w przypadku gazu. Średnia cena gazu na rynku spot na TGE w marcu wyniosła 703,44 zł za MWh, co oznacza wzrost o 320,38 zł na MWh względem lutego 2022 r. i zarazem najwyższą cenę miesięczną w historii tego rynku.

Z kolei na rynku terminowym gazu cena średnia z dostawą w roku 2023 wyniosła w marcu 2022 r. 392,90 zł za MWh, czyli o 108,62 zł na MWh więcej względem analogicznej ceny tego kontraktu w lutym 2022 r.

Tak znaczące wzrosty cen energii elektrycznej, gazu i innych surowców nie są wykluczone w kolejnych miesiącach. Sytuacja na tych rynkach jest rozchwiana, ta niepewność może się zwiększyć po nałożeniu przez UE kolejnych sankcji na Rosję.

Prądu nie zabraknie

Polska, tak jak i wiele innych krajów UE, z Rosji importuje węgiel kamienny, gaz ziemny i ropę naftową – w przypadku tych trzech surowców sytuacja jest inna.

W 2021 r. z Rosji sprowadziliśmy ok. 9 mln ton węgla kamiennego. Co ważne, nie trafia on do polskich elektrowni, lecz do gospodarstw domowych i małych, lokalnych firm i ciepłowni. Ministerstwo Aktywów Państwowych (MAP) zapewnia, że elektrownie kontrolowane przez spółki Skarbu Państwa (czyli przeważająca większość) spalają tylko węgiel z polskich kopalń. Nie ma więc zagrożenia, że z powodu sankcji na węgiel z Rosji zabraknie surowca do polskich elektrowni. Może go jednak zabraknąć dla małych odbiorców. Polskie kopalnie zapowiadają zwiększenie wydobycia węgla, ale na pewno nie uda im się zastąpić całego importu z Rosji. Konieczny więc będzie import węgla z innych kierunków – mówi się o Australii, Indonezji i USA. Od sierpnia 2022 r. ma zostać wprowadzony zakaz importu węgla z Rosji, a do tego czasu można spodziewać się wzrostu importu surowca, aby zrobić jego zapasy.

Koniec z gazem z Rosji

Inaczej jest z gazem ziemnym. W 2021 r. zużycie gazu ziemnego w Polsce wyniosło blisko 20 mld metrów sześciennych, z czego ok. 9,7 mld stanowił import z Rosji. Więc blisko połowa gazu zużywanego w Polsce pochodzi z Rosji. Ta sytuacja ma się zmienić z początkiem 2023 r. Stanie się tak, ponieważ z końcem 2022 r. kończy się obowiązujący kontrakt na zakup gazu z Rosji.

W zamian będziemy kupować gaz z innych kierunków. Jeszcze w październiku 2022 r. ma rozpocząć się przesył gazu rurociągiem Baltic Pipe, który będzie dostarczał surowiec z Norwegii do Polski. Gazociąg Baltic Pipe będzie mógł transportować docelowo 10 mld m sześc. gazu ziemnego rocznie do Polski.

Dodatkowo, w maju 2022 r. ma rozpocząć się przesył gazu do Polski z Litwy gazociągiem GIPL. Rurociągiem będzie można przesyłać do 2 mld m sześc. gazu rocznie.

Nie można zapominać też o dostawach skroplonego gazu LNG do Polski. Obecnie zdolności polskiego terminala pozwalają na import rocznie ok. 5-6 mld m sześc. LNG, ale wkrótce te moce mają wzrosnąć. Do tego dochodzi wydobycie krajowe, wynoszące ok. 4 mld m sześc. rocznie.

Składając te puzzle razem, wychodzi, że pomimo zakończenia kontraktu gazowego z Rosją z końcem 2022 r. w Polsce gazu nie powinno zabraknąć. Inną kwestią pozostaje cena surowca. Ta raczej od obecnych stawek niższa nie będzie...

Dywersyfikacja dostaw ropy

Jeszcze inaczej wygląda sytuacja z ropą. Tutaj jesteśmy zmuszeni na import niemal całego surowca zużywanego w Polsce, krajowe wydobycie ropy jest bardzo niewielkie i wynosi ok. 4 proc. krajowego zapotrzebowania.

Jednym z głównych kierunków importu ropy przez Polskę jest Rosja. Jak podał Polski Instytut Ekonomiczny (PIE), Polska spośród krajów unijnych w latach 2019–2020 była za Niemcami drugim największym importerem ropy naftowej z Rosji.

W 2019 r. sprowadzono do Polski 195 mln baryłek surowca, w tym 133,4 mln baryłek z Rosji (68 proc.), rok później niecałe 183,3 mln baryłek, z czego 131,2 mln baryłek z Rosji (72 proc.).

Obecnie udział rosyjskiej ropy w kontraktach PKN Orlen to ok. 30 proc. Import wynika z umów długoterminowych, których zerwanie, jak zapewnia Orlen, naraziłoby płocki koncern na kary i procesy.

To wszystko oznacza, że już za kilka miesięcy Polska nie będzie importowała z Rosji węgla i gazu, a niewiadomą pozostaje kwestia importu ropy. Na tle niektórych innych krajów UE Polska wygląda całkiem dobrze – już posiada, lub wkrótce będzie posiadać, rozbudowaną infrastrukturę do importu gazu i pracuje nad dywersyfikacją dostaw ropy. ■

IoT JAKO USŁUGA WYMAGA ZAPEWNIENIA BEZPIECZEŃSTWA

KLAUDIA WOJCIECHOWSKA

Rynek Internetu Rzeczy cały czas się rozwija, i to coraz prężniej. Rozwiązania z zakresu IoT stają się usługą – IoT as a Service. Oczywiście niezwykle ważne jest zachowanie bezpieczeństwa przy tej technologii.

Internet Rzeczy jest tematem, o którym mówi się i słyszy coraz więcej. Rynek rozwija się w szybkim tempie. Przywiązanie nas do rozwiązań internetowych przez pandemię sprawiło, że także segment IoT przyspieszył swój rozwój.

Internet Rzeczy pozwala zdalnie wykonywać wiele zadań. Serwisowanie urządzeń czy kontrola nad poszczególnymi z nich lub nad całą infrastrukturą przemysłową to tylko niektóre z możliwości. Zajmujący się rozwiązaniami IoT starają się dostosować swoją ofertę do potrzeb rynku. Najpierw oferowano sprzedaż komponentów pozwalających na budowę tego typu środowisk sieciowych. Później zaczęto oferować pełne systemy. W końcu nastąpił moment sprzedaży IoT jako zintegrowanej usługi.

W zeszłym roku duże firmy wydały na zakup infrastruktury IoT średnio 400 tys. dolarów – tak wynika z badania Gartnera. W tym roku ma nastąpić wzrost tych wydatków o ponad 50 proc. Jak widać, jest to rynek, na którym obroty stale rosną.

Jednak podstawową kwestią jest obecnie bezpieczeństwo przy stosowaniu IoT. Nie jest to sprawa prosta, bo Internet Rzeczy jest systemem wielopoziomowym. Bezpieczeństwo należy zapewnić nie tylko w przypadku punktów końcowych, ale również we wszystkich połączeniach sieciowych oraz w chmurze.

Wymaga to współpracy wszelkich podmiotów odpowiedzialnych za poszczególne elementy systemu. Dostawcy urządzeń odpowiedzialni są za bezpieczeństwo samych urządzeń. Za bezpieczeństwo połączeń odpowiadają dostawcy sieci. Zaplecze zabezpieczają natomiast dostawcy usług chmurowych.

Idealnym rozwiązaniem byłoby zintegrowanie wszystkich tych działań w jednym podmiocie, np. konkretnego dostawcy rozwiązania IoT as a Service. Wtedy zwiększy się szansa na sukces w wyścigu z hakerami, którzy coraz częściej atakują systemy IoT. ■

CHMURA TO TAKŻE PROBLEMY

KLAUDIA WOJCIECHOWSKA

W pandemii praca zdalna okazała się podstawą funkcjonowania wielu z nas. Wtedy też chmura stanowiła technologię, która stała się wybawieniem. Jednak okazuje się, że może ona również sprawiać niemiłe niespodzianki.

Chmura to technologia pozwalająca na innowacyjne zarządzanie firmą i dostarczająca wielu możliwości. Jednak niesie ona ze sobą nie tylko pozytywy, lecz także negatywy – i dobrze zdawać sobie z nich sprawę.

Jedną z niespodzianek może być kwestia opłat. Struktury opłat za usługi sieciowe zostały stworzone z niezwykłą przebiegłością, co może skutkować zaskoczeniem przy otrzymywaniu rachunków. Plany cenowe dla instancji obliczeniowych są tak skomplikowane, że firmy takie jak Apstra stworzyły cały system ich śledzenia. Wymagało to użycia uczących się maszyn wyposażonych w AI. O tej pułapce wiedzieli jednak analitycy, a niektórzy z nich nawet przed tym ostrzegali.

Dostawcy usług chmurowych dają też zespołom DevOps (Development Operations) narzędzia do tworzenia wirtualnych biur w różnych miejscach. A to dodawało pracy chociażby inżynierom sieci, którzy musieli połączyć wszystkie nowe wirtualne domeny. Trudnością był też brak automatyzacji wielu zadań, co wymuszało konfigurowanie zapór i przydzielanie adresów za każdym razem. Dla jednych tworzenie nowego biura to jedno kliknięcie myszy. Dla innych to wiele czasu poświęconego na żmudne zadania. Pracownicy DevOps zyskiwali, inżynierowie sieci na tym tracili.

Technologie chmury i usługi sieciowe to także możliwość rozdzielania zasobów firmy. Jednak odsłanianie powierzchni kolejnych systemów IT to furtka dla cyberprzestępców. Do tego dochodzi niezabezpieczenie różnych aplikacji z usług chmurowych. A to z kolei pokazuje, że zagrożenia cyfrowe przy korzystaniu z chmury są większe niż bez jej udziału.

Żeby sieci korporacyjne w chmurze były bezpieczne, należy wdrożyć czasochłonne działania, które mogą spowalniać przedsiębiorstwo chcące zainwestować w nowe usługi informatyczne dla wsparcia procesów biznesowych lub klientów.

– W swoim podnieceniu branża IT zapomniała, że chmura wymaga nie tylko usług sieciowych, ale także obliczeniowych i pamięci masowej – mówi Ralph Munsen, CIO w Warner Music Group. Oznacza to, że przy korzystaniu z chmury trzeba zatrudniać dodatkowy personel do obsługi problemów, co z kolei skutkuje opóźnieniami. To także zmiana przydziału etatów i budżetów.

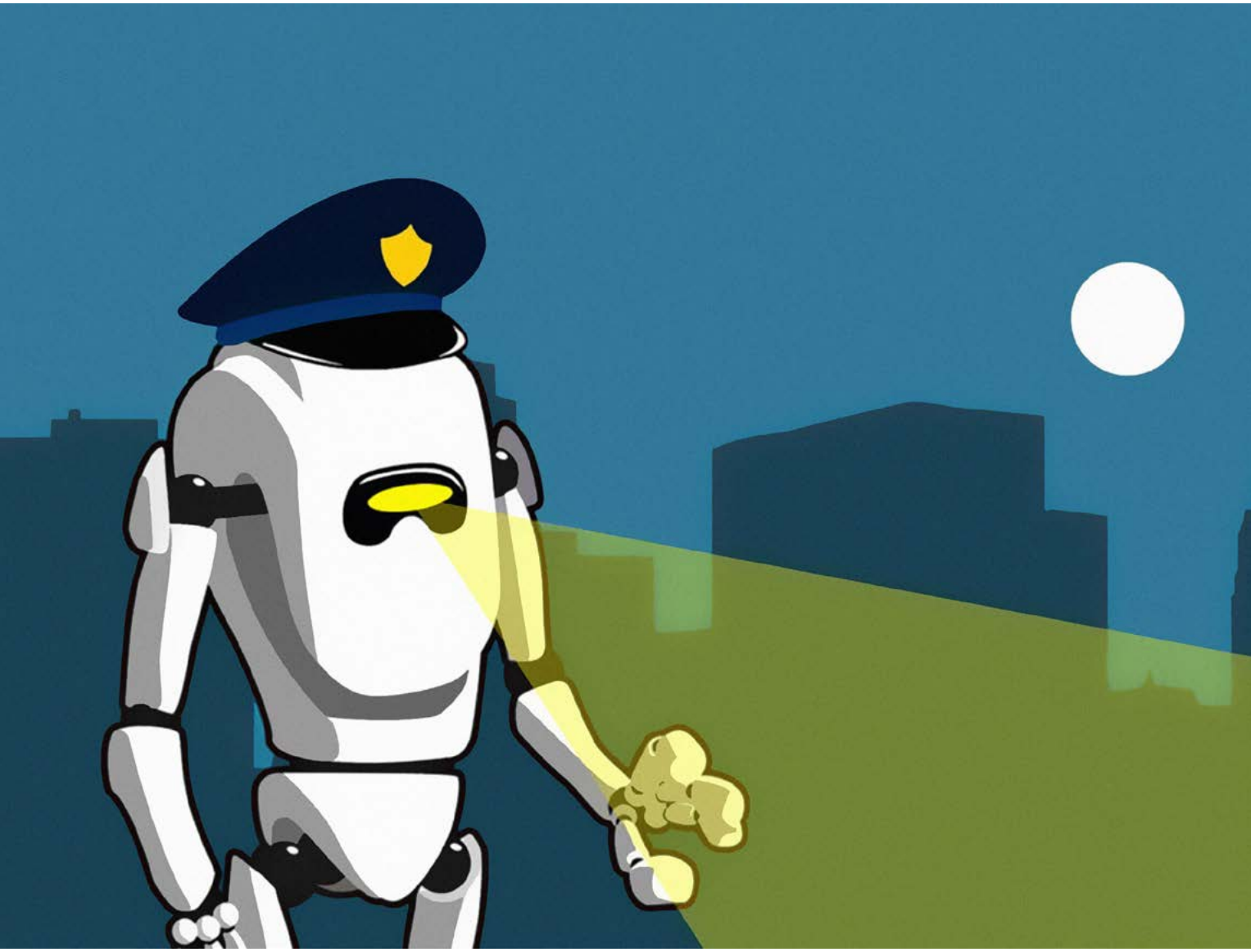
Ogólnie chmura to nie tylko nowe możliwości, ale też nowe problemy, których nie było przed jej pojawieniem się. To zmiana technologiczna i kulturowa. Inny sposób zarządzania i prowadzenia biznesu.

– Prawdę mówiąc, chmura pomaga teraz firmom na nowo wyobrazić sobie, w jaki sposób mogą one kontaktować się ze swoimi klientami – mówi Mohamed Zamzam, szef działu migracji do chmury i usług zarządzanych w BJSS – W wyniku działania chmury powstają nowe modele biznesowe. Są to zmiany, których nadejścia nikt się nie spodziewał – dodaje. ■

KRYMINALNE ZAGADKI AI

MICHAŁ KOCH

W filmie „Raport mniejszości", będącym ekranizacją opowiadania Philipa K. Dicka, bohater grany przez Toma Cruise'a łapie kryminalistów przed popełnieniem przez nich czynu zabronionego. Dzięki wykorzystaniu technologii (i odrobinie SF) policja w tamtym świecie ma dostęp do systemu, który potrafi przewidzieć, kto i kiedy popełni przestępstwo. Zbrodnia praktycznie przestaje istnieć. Czy to też nasza przyszłość?



W latach 60. na terenie Północnej Karoliny grasował seryjny morderca Zodiak. Śledztwo policyjne toczyło się równolegle w kilku departamentach przez lata, a w wyniku utrudnionej łączności (jeden z posterunków nie posiadał nawet faksu!) i braku komunikacji pomiędzy jednostkami nigdy nie udało się złapać mordercy. Tożsamości Zodiaka do dziś nie potwierdzono. W następnych dekadach kryminologię usprawniły komputery, w tym bazy danych i internet. Wkrótce możemy być świadkami kolejnej rewolucji.

Rozwój sztucznej inteligencji to według ekspertów jeden z najgorętszych trendów nadchodzących lat. Już teraz obserwujemy zaawansowane prace nad autonomicznymi pojazdami, a branżę turystyczną ma ulepszyć robot-przewodnik, który, łącząc się z internetem, ma zasypywać towarzyszy podróży ciekawostkami o odwiedzanych miejscach – chiński RoboHon niech posłuży za przykład. Jednakże czy AI może wejść do świata policji i wymiaru sprawiedliwości, by brać udział w sprawach karnych, monitorować podejrzanych i wspomagać prewencję? Wszystko wskazuje, że tak. Prace już trwają.

AI i uczenie maszynowe (ang. machine learning; obszar sztucznej inteligencji poświęcony algorytmom, które poprawiają się automatycznie poprzez doświadczenie) to dwie technologie, które doskonale sprawdzają się w wykrywaniu wzorców możliwych do przeoczenia przez ludzi. Wykorzystują algorytmy do analizy ogromnych zbiorów danych w celu znalezienia najlepszego rozwiązania i prognozowania wyników zdarzeń. Co najważniejsze – czynią to w bardzo krótkim czasie.

Analiza predykcyjna, wynikająca z pracy algorytmów, już pozwala na ocenę ryzyka podczas procesu karnego. Sędziowie zwracają się o przygotowanie analizy, która pomaga ocenić, czy podejrzany może zostać zwolniony za kaucją lub czy istnieją przesłanki do zwiększenia poziomu zabezpieczeń na sali sądowej podczas rozprawy.

Naukowcy z Uniwersytetu Leon w północno-zachodniej Hiszpanii przeszkolili sieć neuronową, aby wykrywała ślady pozostawione na miejscu zbrodni. Przyjęli, że poprzez przesłanie tysięcy obrazów z miejsc przestępstw do komputera, czyli de facto dzięki wykorzystaniu zalet uczenia maszynowego, algorytmy „nauczą" się wzorców do wykrycia. Sprawi to, że śledczy będą mogli sprawdzić, czy seria włamań to dzieło jednej osoby albo grupy przestępców. Innym rozwiązaniem jest oznaczanie przez sztuczną inteligencję wybranych przedmiotów lub zdarzeń na dostarczanych zdjęciach. System wskazuje np. odciski butów, a także łączy je z konkretnym modelem figurującym w bazie danych.

Identyfikowanie podejrzanych przez algorytmy na podstawie zdjęć to kolejna stosowana już metoda. Technologia jest wykorzystywana przez organy ścigania na całym świecie do sprawdzania tożsamości osób zarówno w internecie, jak i w świecie realnym. Po wprowadzeniu zdjęcia podejrzanego do bazy danych możemy odszukać go na setkach tysięcy stron internetowych. Ręczne sprawdzenie takich zasobów byłoby niewykonalne.

AI i uczenie maszynowe to dwie technologie, które doskonale sprawdzają się w wykrywaniu wzorców możliwych do przeoczenia przez ludzi. Wykorzystują algorytmy do analizy ogromnych zbiorów danych w celu znalezienia najlepszego rozwiązania i prognozowania wyników zdarzeń.

Do zalet omawianego rozwiązania zatem trzeba zaliczyć obniżenie kosztów prowadzonego śledztwa. Wcześniej funkcjonariusze musieli spędzać niezliczone godziny na analizowaniu miejsca przestępstwa, nagrań z kamer bezpieczeństwa, akt dowodowych i wielu innych rzeczy, aby złapać podejrzanych. Dzięki rozwojowi AI wszystko to można zrobić szybciej, taniej i bardziej wydajnie.

Wykrywanie przestępstw dzięki technologii to sprawa znana w bankowości. Instytucje finansowe od dziesięcioleci używają systemów monitorowania transakcji, ale wymaga to od nich sprawdzania otrzymanych rezultatów. Wyniki nie są oszałamiające: wskazuje się, że tylko 2 proc. transakcji oznaczanych przez systemy jako przestępstwa okazuje się nimi w rzeczywistości. Obecność nowoczesnych algorytmów sprawia też, że oczekujemy natychmiastowej reakcji przez platformy social mediowe w przypadku, gdy opublikowany zostanie na nich film sprzeczny z prawem lub normami społecznymi.

W świecie, w którym obok ludzi istnieje rozwinięta sztuczna inteligencja, prędzej czy później należałoby się też zastanowić, czy AI również zdolna jest do popełniania przestępstw. Temat poruszany jest wielokrotnie przez literaturę SF (m.in. wspomniany Philip K. Dick, ale też Isaac Asimov, twórca etyki robotów). Na szczęście obecnie to bardziej fiction niż science.

Sztuczna inteligencja i jej analizy predykcyjne są przyjmowane przez entuzjastów jako mogące polepszyć niesprawny system sądownictwa karnego. Jednak wielu ekspertów prawnych, technologów i działaczy społecznych uważa, że te narzędzia mogą w rzeczywistości zaostrzyć problemy, które teoretycznie mogłyby rozwiązywać. Interesująco wyglądałaby też sama rozprawa, gdyby podejrzany został oskarżony na podstawie danych zebranych przez algorytmy. Czy w imię zasady domniemania niewinności twórcy danego programu AI musieliby zdradzić jego tajniki, aby przedstawić metodologię, na podstawie której dokonano identyfikacji sprawcy?

Obecna technologia pozwala na wiele. Jednakże wciąż daleko nam do sytuacji z „Raportu mniejszości". Zresztą nie sądzę, byśmy kiedykolwiek osiągnęli ten poziom, zwłaszcza że skazywanie przestępców opiera się zarówno na czynnościach śledczych i procesowych, jak i na doktrynalnych przepisach prawa karnego. Pracy sztucznej inteligencji przy selekcjonowaniu podejrzanych zawsze będzie musiał zatem przyglądać się człowiek. ■

SZTUCZNA INTELIGENCJA NA POLU BITWY

KLAUDIA WOJCIECHOWSKA

Amerykańska agencja oraz NATO pracują nad „cyfrowymi asystentami". Ich zadaniem ma być przede wszystkim segregacja rannych na polu walki. Może to ocalić życie wielu ludziom.

DARPA to Agencja Departamentu Obrony ds. Zaawansowanych Projektów Badawczych, która już w 2018 roku przeznaczyła dwa miliardy dolarów na rozwój sztucznej inteligencji. Program o nazwie AI Next obejmował ponad 60 „projektów obronnych".

Teraz DARPA pracuje nad planem stworzenia AI podejmującej szybkie decyzje w trudnych sytuacjach. Program nazwano In the Moment (ITM). Ma on znaleźć zastosowanie na polu walki czy w przypadku zamachów. W założeniu będą to takie sytuacje, w których człowiek nie jest w stanie jednoznacznie podjąć dobrej decyzji. Wtedy do akcji wkraczają asystenci AI.

Ich funkcjonowanie będzie oparte na algorytmach wykorzystujących umiejętności segregowania rannych w przypadkach masowych ofiar. Dodatkowo będą posiadały one dostęp do ogromnej bazy danych, takich jak zasoby najbliższych szpitali. To wszystko pozwoli im podejmować lepsze decyzje.

DARPA przewiduje rozwijanie programu przez trzy i pół roku. Podzielony będzie on na dwie fazy. W trakcie prac fachowcy mają oceniać decyzje podejmowane przez AI i ludzi, by wskazać, czyje lepiej sprawdzają się w sytuacjach wyjątkowych.

Podobną technologię opracowuje NATO. Dziennik The Washington Post podał, że Sohrab Dalal, pułkownik i szef wydziału medycznego Naczelnego Dowództwa Sojuszniczych Sił NATO ds. Transformacji, kieruje zespołem projektującym „cyfrowego asystenta triażu" (umiejętności segregowania rannych).

Prace DARPY nad AI nie ograniczają się do samego projektu nad wykorzystaniem jej we wskazanym zastosowaniu. W ramach programu Air Combat Evolution sprawdzają oni także skuteczność sztucznej inteligencji w powietrznych walkach zespołowych. ■

Pełną listę programów agencji można znaleźć na stronie:

https://www.darpa.mil/work-with-us/ai-next-campaign

JAMBOX

www.jambox.pl

tv smart

DEKODERY IPTV
Arris 4302 HD
Arris 5305 4K

CatchUp
7 DNI WSTECZ

StartOver
OGLĄDAJ OD POCZĄTKU

JAMBO Nagrywarka
NAGRYWAJ W CHMURZE

ZAMÓW TERAZ NA BEZPŁATNE TESTY
sgt.net.pl

NOWOŚĆ!

TV Smart 4K BOX to dekoder z Android TV, który łączy tradycyjną telewizję z dostępem do serwisów rozrywkowych, takich jak: Netflix, HBO Max, Viaplay, Amazon Prime oraz ogromnej biblioteki VOD.

TV Smart to także:
- Telewizja linearna z funkcjami: StartOver, CatchUp, Nagrywarka w chmurze
- Pilot bluetooth z możliwością głosowej obsługi
- Możliwość instalacji aplikacji Android TV
- Wbudowane Wi-Fi i Chromecast

TELEFONIA KOMÓRKOWA
JAMBOX mobile
LTE 5G

Blisko **300** kanałów, w tym **182** w jakości HD i **5** UHD 4K
Atrakcyjna oferta pakietowa

4K HD EPG VOD PVR TIME SHIFT MULTI SCREEN JAMBOX GO! JAMBO NAGRYWARKA START OVER CATCH UP

- 15 lat na rynku IPTV, 350 partnerów ISP
- 103 tys. abonentów JAMBOX
- Nowoczesne autorskie oprogramowanie HD dekoderów
- Zaawansowany system zarządzania usługami
- Dystrybucja usługi w multicast i unicast
- Wsparcie marketingowo-sprzedażowe
- **JAMBOX go!** – oglądanie TV i zarządzanie usługami ze smartfona, komputera czy tabletu
- **JAMBOX mobile** – telefonia i internet 5G i LTE, proste przenoszenie numerów, taryfy pracownicze

SGT

Pomagamy lokalnym operatorom Internetu wdrażać w swoich sieciach cyfrową telewizję kablową bazującą na platformie IPTV oraz telefonię komórkową i Internet LTE.

sgt.net.pl/iptv-dla-isp

Zadzwoń lub wyślij email

32 428 8 428 handlowy@sgt.net.pl

CZY NADCHODZI KONIEC TELEWIZJI SATELITARNEJ?

KLAUDIA WOJCIECHOWSKA

Kilkanaście lat temu to telewizja satelitarna pozwalała na dostęp do dużej liczby kanałów z Polski i ze świata. Platformy cyfrowe inwestowały w nowe kanały i w ten sposób przyciągały abonentów. Teraz w USA wyraźnie widać spadek zainteresowania platformami satelitarnymi, a eksperci mówią o tym, że trend dociera również do Polski.

W Polsce operatorzy płatnych telewizji zyskiwali przez opóźnienie wprowadzenia naziemnej telewizji cyfrowej. Ponadto w mniejszych miejscowościach nie działały sieci kablowe. Jedynym sposobem na korzystanie z szerszej oferty niż stacje TVP dla wielu osób było podpisanie umowy z operatorem cyfrowym (Cyfrowym Polsatem czy Cyfrą+). Pozwoliło tym firmom na zdobycie wielu milionów abonentów.

Po uruchomieniu naziemnej telewizji cyfrowej rozwój platform cyfrowych spowolnił. Jednak na razie nie nastąpił jeszcze wyraźny odpływ klientów, jednak sytuacja w USA pokazuje, że także u nas może to nastąpić.

Prezes amerykańskiej platformy satelitarnej Dish Network – Charlie Ergen potwierdził, że jego firma w ciągu kwartału straciła 273 tys. abonentów. W sumie z 13 mln klientów 5 lat temu spadła do 8 mln obecnie. Uznał, że tylko fuzja z DirecTV jest w stanie uratować obie firmy. Platforma DirecTV także odnotowuje spadek liczby abonentów z 25 mln w 2017 roku do 15 mln obecnie.

Chociaż pierwsze rozmowy o fuzji Dish Network i DirecTV pojawiły się 20 lat temu, to wtedy urząd antymonopolowy nie zgodził się na połączenie platform. Teraz przy spadku zainteresowaniem obiema platformami powody uznane za podstawę odmowy już nie istnieją.

Obecnie na amerykańskim rynku królują platformy streamingowe takie jak Netflix, Amazon Prime Video, Disney+ HBO Max, Discovery+.

Podobna sytuacja ma już miejsce w Europie. Platformy Sky w Wielkiej Brytanii, Niemczech i we Włoszech w samym 2021 r. straciły w 2021 198 tys. abonentów.

W Polsce Canal+ od 2020 roku nie podaje liczby abonentów. Polsat Box w raportach operuje liczbą sprzedanych usług.

Wgląd w sytuację mogą dać dane z Orange. W 2021 r. firma miała 995 tysięcy klientów usług telewizyjnych. Z czego 710 tys. to byli klienci IPTV, a 285 tys. – satelitarni. O ile w pierwszej grupie nastąpił wzrost o 41 tys., to w drugiej spadek wyniósł 54 tys.

– Platformy satelitarne okres świetności mają za sobą. Swego czasu stanowiły rzeczywiście najszybszy sposób na dostarczenie dobrej jakości sygnału telewizyjnego tam, gdzie nie nadążała infrastruktura kablowa i telekomunikacyjna. Dlatego głównym konkurentem platform satelitarnych były szybko rosnące sieci telewizji kablowej, posiadające istotną przewagę w postaci tzw. potrójnej usługi (telewizja/internet/telefon) – zauważa w rozmowie z Wirtualnemedia.pl Marek Sowa, przewodniczący Rady Nadzorczej Golf Channel Polska, a wcześniej prezes Agory i wiceprezes sieci kablowej UPC Polska.

Lepszą sytuację można zauważyć w sieciach kablowych. Oprócz telewizji oferują one bowiem dostęp do szerokopasmowego internetu. Bez tego nie można korzystać z platform streamingowych.

– O ile jednak sieci telewizji kablowej i telekomy od dawna stawiają na szerokopasmowy dostęp do Internetu, tym samym zabezpieczając się przed „odcinaniem kabla" przez klientów, platformy satelitarne samodzielnie nie mają zbyt wielu atutów w starciu z platformami streamingowymi. W miarę rozwoju infrastruktury internetowej, platformy satelitarne zaczynają tracić klientów, szybciej w miastach, wolniej w mniejszych ośrodkach – wyjaśnia Marek Sowa.

Jednak także w małych miasteczkach i na wsiach ta sytuacja zmieni się dzięki rozwojowi sieci 5G. Nie będzie limitów transferów danych, które utrudniają korzystanie ze streamingu. To może oznaczać koniec platform satelitarnych. ■

MIKROTIK ROUTEROS7 JAKO ROUTER BGP

IHOR HRESKIV

Urządzenia łotewskiej firmy MikroTik, bardzo popularne wśród domowych użytkowników lub w małych i średnich przedsiębiorstwach, nie zdobyły czołowego miejsca jako routery brzegowe w sieciach ISP. Było to związane z ograniczeniami jądra systemu operacyjnego Linux używanego w wersji 6 systemu RouterOS. Niestety wersja ta nie pozwalała na wydajne wykorzystanie wielu rdzeni procesora przez protokoły routingu dynamicznego.

Najnowsza wersja ROS7 ma zupełnie inne podejście do całego podsystemu routingu, przez co pozwala na znaczne przyspieszenie obsługi protokołów routingu dynamicznego. To w połączeniu z nowymi modelami urządzeń serii CCR (m.in. CCR2004, CCR2116) działającymi na architekturze ARM 64 bit ponownie skupiło uwagę administratorów z segmentu ISP na rozwiązania łotewskiego producenta do zastosowań jako routery BGP.

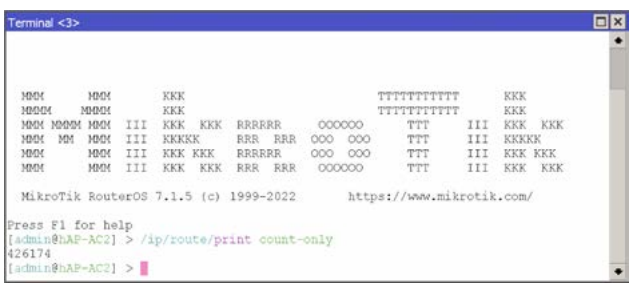
W tym artykule postaram się wskazać, jak wiele się zmieniło, i mam nadzieję, że wielu z was znajdzie tu argumenty przemawiające za wykorzystaniem ROS7 w waszych infrastrukturach.

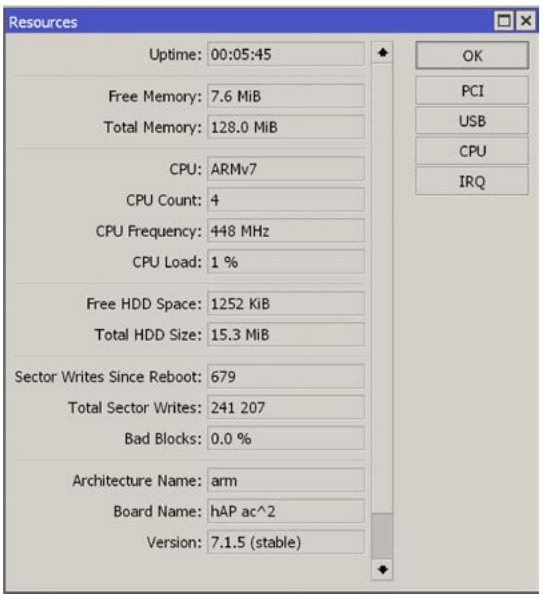
Poniższy wykres przedstawia widok pochodzący z systemu monitorowania Zabbix. Możemy zauważyć ogromną różnicę w wykorzystaniu zasobów procesora, przy takiej samej ilości tras dodanych do routera za pośrednictwem protokołu BGP.

Na podanych wykresach testy przeprowadzone zostały na urządzeniu MikroTik CHR (Cloud Hosted Router) używającym systemu RouterOS wersjach 6.49.5 oraz 7.1.5. Na każdym z tych routerów jest po jednym połączeniu do jednego peera z tak zwanym „full feed", czyli pełną tablicą routingu „całego internetu", która w kwietniu 2022 roku liczyła około 910 tysięcy wpisów.

Jako ciekawostkę warto tutaj wspomnieć o najbardziej popularnym urządzeniu segmentu SoHo, czyli MikroTik hAP AC².

Na tym routerze również można zestawić jednego peera z „full feed" BGP. Na tym urządzeniu tablica routingu instaluje się w 57 sekund.





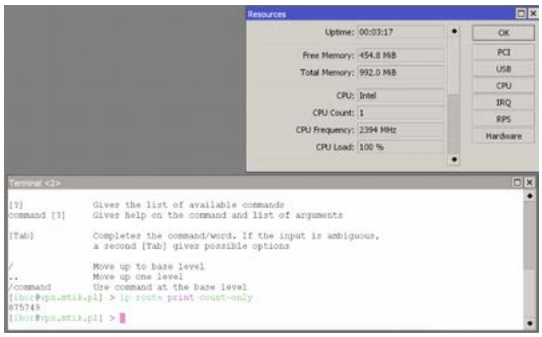
Na powyższych zrzutach ekranu można zaobserwować liczbę wpisów po filtracji oraz wykorzystanie zasobów routera. I chociaż ciężko sobie wyobrazić praktyczne użycie tego routera w środowisku produkcyjnym, przykład ten obrazuje, jak wiele zmieniło się w sposobie obsługi BGP w RouterOS 7.

System operacyjny MikroTik RouterOS 7 wspiera BGP Version 4, zgodnie ze standardem RFC 4271. Oprócz tego wspierane są poniższe standardy:

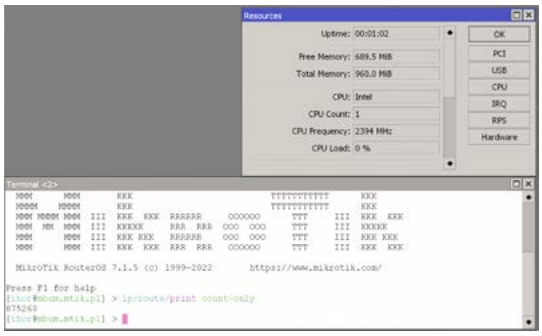
RFC 4271	Border Gateway Protocol 4
RFC 4456	BGP Route Reflection
RFC 5065	Autonomous System Confederations for BGP
RFC 1997	BGP Communities Attribute
RFC 8092	BGP Large Communities
RFC 4360, 5668	BGP Extended Communities
RFC 2385	TCP MD5 Authentication for BGPv4
RFC 5492	Capabilities Advertisement with BGP-4
RFC 2918	Route Refresh Capability
RFC 4760	Multiprotocol Extensions for BGP-4
RFC 2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
RFC 4893	BGP Support for Four-octet AS Number Space
RFC 4364	BGP/MPLS IP Virtual Private Networks (VPNs)
RFC 4761	Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signalling
RFC 6286	AS-wide Unique BGP Identifier for BGP-4

Zmiana jądra Linux na wersję 5.x dała możliwość obsługi protokołów routingu na wszystkich rdzeniach dostępnych w systemie. Oprócz tego cały podsystem routingu nie został przebudowany, jak to się odbywało dotychczas, a napisany zupełnie od nowa. Miało to na celu bardziej optymalne wykorzystanie RAM-u oraz zasobów CPU, co widać na poniższych zrzutach ekranu.

ROS6

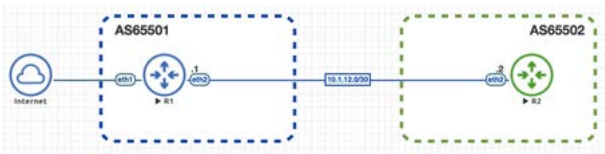


ROS7



Przedstawię teraz, jak skonfigurować peering pomiędzy dwoma lokalizacjami przy użyciu protokołu BGP. Ponieważ tak jak wspomniałem wcześniej system RouterOS został napisany od zera, tak i konfiguracja tego procesu będzie znacząco różna od tego, jak byliśmy przyzwyczajeni do konfigurowania w RouterOS 6.

Schemat sieci.



Opuścimy konfigurację wstępną, czyli między innymi: adresowanie interfejsów, nadawanie nazw routerom oraz zagadnienia związane z bezpieczeństwem.

Na routerze R1

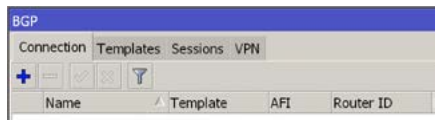
```
/routing/bgp/connection
add name=peer-to-R2 remote.address=10.1.12.2 as=65501\ local.
role=ebgp
```

Na routerze R2

```
/routing/bgp/connection
add name=peer-to-R1 remote.address=10.1.12.1 as=65502\ local.role=ebgp
```

```
[admin@R1] > routing/bgp/session/print
Flags: E - established
 0 E remote.address=10.1.12.2 .as=65502 .id=10.1.12.2 .refused-cap-opt=no
     .capabilities=mp,rr,gr,as4 .messages=9 .bytes=171 .eor=""
     local.address=10.1.12.1 .as=65501 .id=10.1.12.1 .capabilities=mp,rr,gr,as4 .messages=9
     .bytes=171 .eor=""
     output.procid=20
     input.procid=20 ebgp
     hold-time=3m keepalive-time=1m uptime=0m4s120ms
```

Po nawiązaniu połączenia po protokole BGP możemy obserwować w zakładce „Sessions" zestawioną sesję do R2.



Dla propagowania/rozgłaszania użyjemy dwóch prefiksów 172.16.0.0/24 i 172.17.0.0/24 z AS65001 do innych systemów autonomicznych. W tym przypadku mamy tylko jednego peera R2, który należy do AS65502. W nowej implementacji nie ma już zakładki „Networks" dla rozgłaszania prefiksów. W RouterOS 7 należy skorzystać z zakładki „Address List" ip/firewall, gdzie tworzy się listę prefiksów.

W RouterOS 7 protokół BGP będzie propagować tylko te prefiksy, dla których znajdują się wpisy w tablicy FIB (Forwarding Information Base). Każdą z tych sieci utworzymy w inny sposób.

Dla pierwszej sieci stworzymy interfejs typu bridge pełniący rolę aktywnego interfejsu, który jest zaadresowany 172.16.0.1/24. Dla takiego wpisu pojawi się wpis w tablicy routingu jako aktywny oraz bezpośrednio podłączony.

```
/interface/bridge/add name=loop0
/ip address/add address=172.16.0.1/24 interface=loop0
```

Dla propagacji prefiksu 172.17.0.0/24 utworzymy ręcznie wpis w tablicy routingu typu blackhole.

```
/ip/route
add blackhole disabled=no dst-address=172.17.0.0/24
```

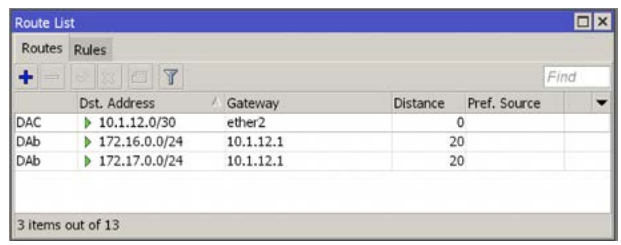
Teraz dodamy wpisy do firewalla do listy adresów z nazwą bgp-distribution:

```
/ip firewall address-list
add address=172.16.0.0/24 list=bgp-distribution
add address=172.17.0.0/24 list=bgp-distribution
```

Zmodyfikujemy wpis do peera R2 na routerze R1 dla wysyłania listy prefiksów:

```
/routing/bgp/connection/set 0 output.network=bgp-distribution
```

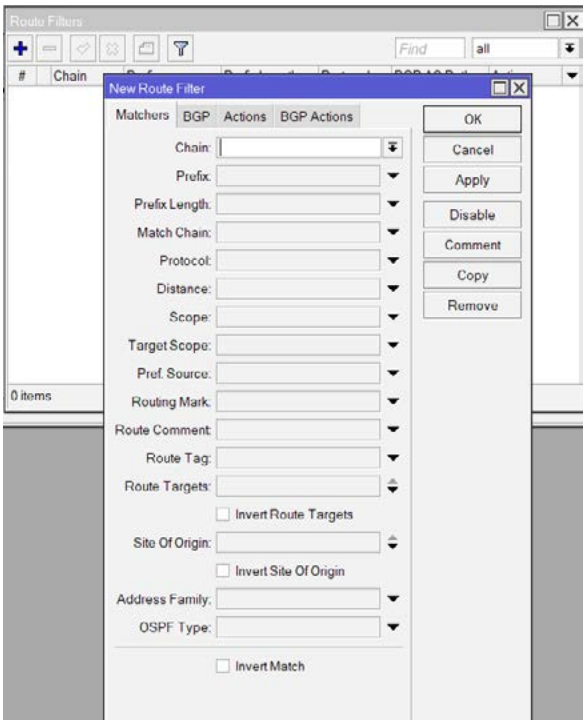
Po zastosowaniu zmian na routerze R2 tablica routingu wygląda następująco.

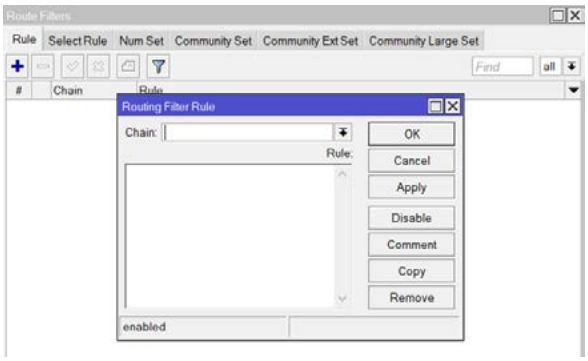


Możemy podejrzeć dwa prefiksy propagowane z routera R1.

Sposób konfiguracji peeringu BGP to tylko jedna ze zmian w implementacji w nowej wersji OS. W tym artykule wspomnę także o bardzo ważnej zmianie, tj. tworzeniu filtrów Routing->filters.

RouterOS7 przyniósł także nowy, w pełni przebudowany system filtrowania tras routingu. Zastąpiono przypominające IP Firewall GUI na okienko typu text area.





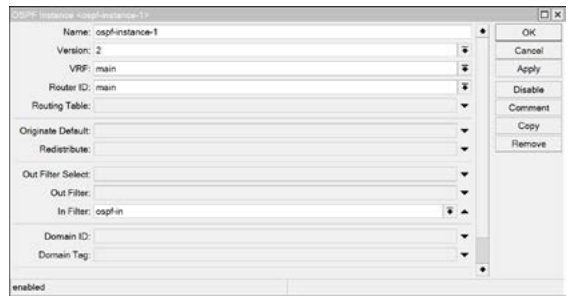
Przy pierwszym zetknięciu z tą zmianą można ją odebrać jako krok wstecz, a nawet znaczne utrudnienie w pracy. Po pewnym czasie administrator zauważy jednak, jak wiele możliwości daje takie podejście.

W polu tekstowym należy utworzyć filtr, wykorzystując coś w rodzaju języka skryptowego. Pełny opis parametrów znajduje się w dokumentacji (nowej, dostępnej pod adresem https://help.mikrotik.com). Najogólniej mówiąc, parametry dzielimy na „tylko do odczytu" (read-only) oraz takie, które mogą posłużyć do wykonania czynności/modyfikacji (writeable). Wszystkie, bez względu na typ, mogą zostać wykorzystane do określenia, jakie trasy mają podlegać regule filtra.

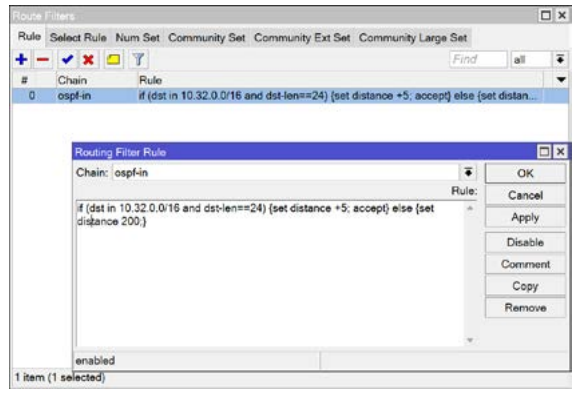
Jednym z prostszych przykładów, jakie przychodzą mi do głowy, obrazującym nowy sposób definicji filtrów, to zmiana wartości distance oraz akceptacja/odrzucenie pewnych prefiksów w OSPF (domyślną akcją każdego z filtrów jest „reject").

❶ W konfiguracji instancji OSPF podajemy nazwę łańcucha weryfikowanego podczas przyjmowania tras.

```
(
konfiguracja CLI OSPF:
/routing ospf instance
add disabled=no in-filter-chain=ospf-in name=ospf-instance-1
/routing ospf area
add disabled=no instance=ospf-instance-1 name=backbone
/routing ospf interface-template
add area=backbone disabled=no interfaces=vlan-2101 networks=10.21.1.0/24
)
```



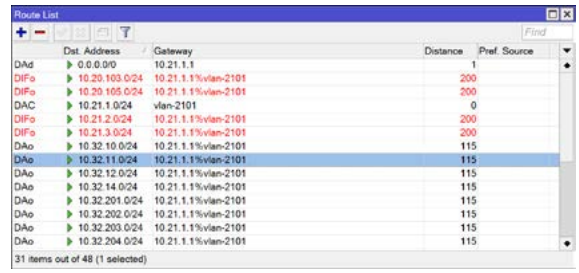
❷ Tworzymy regułę we wcześniej nazwanym łańcuchu.



Polecenie do utworzenia filtru w CLI:

```
/routing filter rule
add chain=ospf-in disabled=no rule="if (dst in 10.32.0.0/16 and dst-len==24) {set\
\_distance +5; accept} else {set distance 200;}
```

❸ W wyniku działania reguły trasy spełniające wymagania wyrażenia warunkowego zmieniły wartość distance, zwiększając ją o 5. Trasy niepasujące zostały odrzucone (domyślna akcja to reject), a także zmieniono im wartość distance na 200.



Już tak prosty przykład pokazuje moc tego rozwiązania dzięki możliwości budowania wyrażeń warunkowych typu if-else.

Ostatecznie, pomimo pewnej dodatkowej porcji wiedzy, jaką administratorzy będą zmuszeni przyswoić, zwiększenie elastyczności kreowania filtrów należy z pewnością zapisać na plus RouterOS7.

Na tym zakończę prezentowanie zmiany do podejścia w konfiguracji na nowym systemie operacyjnym od firmy MikroTik. Głównym wnioskiem artykułu jest to, że nowe podejście do implementacji protokołu BGP w ROS7 ma bardzo pozytywny wpływ na zużycie zasobów routera.

Obecnie należy zadać sobie pytanie, czy już czas na wykorzystywanie ROS7 w środowisku produkcyjnym? Niestety nie ma tutaj jednoznacznej odpowiedzi i jak zawsze ROS7 nadal ma pewne bolączki wieku dziecięcego. Niemniej, w okresie około dwóch miesięcy nie zaobserwowałem problemów ze stabilnością działania BGP ROS7. ■

Ihor Hreskiv

Administrator i architekt systemów informatycznych z ponad 20-letnim doświadczeniem. Studiował na Politechnice w Tarnopolu (Ukraina) na kierunku Programowanie systemów automatyki przemysłowej. Certyfikowany trener MikroTik w MikroTik Warsaw Training Center. Prywatnie uwielbia podróże oraz snookera.

SIECI ŚWIATŁOWODOWE

Część 12 – Ciekawostki i nietypowe instalacje

MICHAŁ ANDRZEJEWSKI

Zapraszamy do lektury ostatniej części cyklu, w której przedstawiony zostanie zbiór ciekawostek i nietypowych instalacji dla sieci światłowodowych.

„Wdmuchiwanie" wodą

Metodą wdmuchiwania kabli, o którą dość często pytają klienci, jest „wdmuchiwanie" wodą. Doświadczenia pochodzące głównie z krajów niemieckojęzycznych oraz Skandynawii wskazują wyraźnie na to, że technika „wdmuchiwania" wodą może być stosowana w szczególnych przypadkach, w zasadzie tylko tam, gdzie najważniejszym kryterium jest duża odległość.

Zalety:

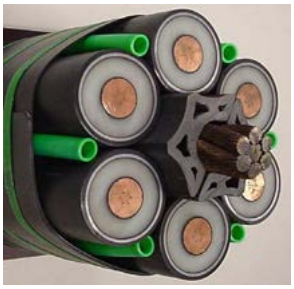
1. Możliwość osiągnięcia dużych odległości w jednym odcinku (do 10 km), tam gdzie nie ma możliwości zrobienia studni pośredniej.
2. Zniwelowanie wpływu wysokich temperatur otoczenia (kraje pustynne).
3. Możliwość wykorzystania standardowych maszyn z niewielkimi modyfikacjami.

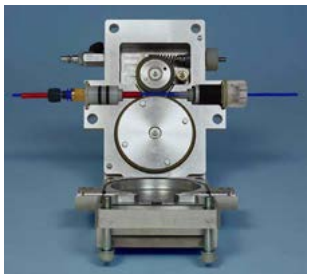
Wady:

1. Większy nakład pracy przy projektowaniu i uzyskiwaniu pozwoleń (władze wodne, ochrona środowiska).
2. Niedopuszczalne są duże różnice poziomów powodujące znaczny wzrost ciśnienia hydrostatycznego.
3. Konieczność stosowania rur osłonowych o większych średnicach, a także o większej wytrzymałości (ze względu na duże ciśnienie wody „wdmuchującej" do 25 barów).
4. Konieczność stosowania pomp ciśnieniowych do wody o ciśnieniach do 25 barów i wydajności uzależnionej od średnic rur osłonowych.
5. Dużo mniejsza prędkość „wdmuchiwania". Większy nakład pracy przy organizacji placu budowy.

W konkretnym testowym przypadku w Niemczech dokonano „wdmuchiwania" wodą mikrokabla D= 6,1 mm w mikrorurkę 10 X 1, gdzie uzyskano odległość 5400 metrów. Proces trwał jednakże aż 5 godzin i 20 minut, czyli średnia prędkość „wdmuchiwania" wyniosła około 17 m/min. W trakcie pracy zużyto około 450 l wody, podawanej przez pompę pod ciśnieniem 22 barów.

Innym przykładem z konkretnej budowy jest projekt zrealizowany w Holandii, gdzie w potężnym kablu energetycznym ułożonym na dnie zatoki Westerschelde umieszczono sześć rurek osłonowych 25/20 pod światłowód.





Kabel do zainstalowania miał średnicę 6 mm i zawierał 49 włókien. Przy użyciu specjalnej maszyny podobnej konstrukcyjnie do MicroJeta firmy Plumett udało się „wdmuchnąć" kabel wodą pod ciśnieniem na odległość 5500 m. Operacja była mocno skomplikowana i wymagała specjalnych przygotowań, ale pokazała, że osiągnięcie takich odległości jest możliwe.

Do „wdmuchiwania" wodą potrzebne jest duże doświadczenie operatorów i doskonała organizacja placu budowy. Nie poleca się stosowania tej technologii firmom zaczynającym swoją pracę przy układaniu sieci światłowodowych. Trzeba wyraźnie zaznaczyć, że jeśli wystąpiły problemy z wdmuchiwaniem kabla powietrzem, to „wdmuchiwanie" wodą też będzie skazane na niepowodzenie.

SENSO JET

SENSO JET

Ta ciekawa technologia została opracowana przez firmę Plumettaz na potrzeby wdmuchiwania kabli sygnalizacyjnych w stalowe rurki osłonowe wzdłuż kabli energetycznych, gazociągów czy innych ważnych rurociągów. Oczekiwane są rezultaty zasięgów rzędu 10 km. W czasie prób laboratoryjnych przeprowadzonych z użyciem wody lub alkoholu osiągnięto zasięgi do 3 km. Średnice stalowych rurek osłonowych wynosiły od 2 do 5 mm, ciśnienie wody 20-40 barów, a ciśnienie alkoholu dochodziło do 100 barów.

BOP (Bytes in old pipes)

Ciekawym zastosowaniem technologii wdmuchiwania kabli światłowodowych jest opatentowane rozwiązanie „Bytes in old pipes", gdzie włókna światłowodowe są wdmuchiwane w mikrorurki umieszczone w rękawie renowacyjnym, którym naprawiono przewód kanalizacyjny.

Wdmuchiwanie długich odcinków światłowodów

Coraz częściej operatorzy sieci teletechnicznych zastanawiają się, jak wdmuchnąć maksymalnie długie odcinki kabla światłowodowego bez konieczności spawania. Mając do dyspozycji odpowiedni sprzęt i doświadczone ekipy instalatorów, bez większych problemów można zainstalować odcinki kabla długości około sześciu kilometrów. Tę operację można przeprowadzić na kilka sposobów, angażując, w zależności od możliwości, więcej sprzętu lub więcej ekip.

Pierwszy sposób jest następujący: stawiamy bęben z kablem (na stojakach lub przyczepie) w środku trasy, zakładając, że w każdą stronę wdmuchniemy po 3 km podzielone na odcinki po 1,5 km. Mamy więc cztery odcinki po 1,5 km i pięć studni, które numerujemy kolejno od lewej strony. Przy użyciu wdmuchiwarki i kompresora wdmuchujemy pierwszy odcinek od studni nr 3 do studni nr 4. Następnie „przedmuchujemy" kabel dalej, układając go przy studni nr 4 na folii w „ósemki" lub zwijając w specjalnym przyrządzie o nazwie Twister. Z kolei przy studni nr 3 odwijamy do drugiego Twistera (lub ósemkujemy na folii) resztę kabla, jaki pozostał na bębnie. Wdmuchujemy kabel od studni nr 3 do studni nr 2 i tam „przedmuchujemy" kolejne 1,5 km do trzeciego Twistera lub „ósemkujemy". Po odwróceniu zwoju kabla, tak, aby dostać się do jego końca, przestawiamy wdmuchiwarkę do studni nr 4 i dmuchamy kabel do studni nr 5. Następnie przestawiamy wdmuchiwarkę do studni nr 2, odwracamy zwój kabla i wdmuchujemy kabel od studni nr 2 do studni nr 1. Praca zakończona przy udziale jednej ekipy wyposażonej we wdmuchiwarkę i kompresor, ewentualnie jeszcze w trzy Twistery.

Drugi sposób można zastosować, jeśli dysponujemy wieloma wdmuchiwarkami i kompresorami oraz ludźmi do ich obsługi. Początek wygląda tak samo. Stawiamy bęben z kablem (na stojakach lub przyczepie) w środku trasy, zakładając, że w każdą stronę wdmuchniemy po 3 km podzielone na odcinki po 1,5 km. Mamy więc cztery odcinki po 1,5 km i pięć studni, które numerujemy kolejno od lewej strony. Przy użyciu wdmuchiwarki i kompresora wdmuchujemy pierwszy odcinek od studni nr 3 do studni nr 4. W studni nr 4 stawiamy kolejną wdmuchiwarkę oraz kompresor i „kaskadowo" dmuchamy dalej kabel do studni nr 5. Połowa pracy wykonana! Następnie przy studni nr 3 odwijamy do Twistera (lub ósemkujemy na folii) resztę kabla, jaki pozostał na bębnie, po czym wdmuchujemy kabel od studni nr 3 do studni nr 2. W studni nr 2 stawiamy kolejną wdmuchiwarkę oraz kompresor i „kaskadowo" dmuchamy dalej kabel do studni nr 1. Praca zakończona przy udziale dwóch ekip wyposażonych we wdmuchiwarkę i kompresor każda. Potrzebny był także wariantowo jeden Twister. ■

BOP (Bytes in old pipes)

METAWERSUM. PROBLEMY I KORZYŚCI

MICHAŁ KOCH

Gdy w 2021 roku Mark Zuckerberg, szef Facebooka, ogłosił, że firma zmienia nazwę i zamierza wyznaczać nowe granice w wirtualnym świecie, zachwycił się również świat realny. Meta, bo tak teraz nazywa się korporacja, chce sprawić, że przeniesiemy znaczną część naszego życia do cyberprzestrzeni. Do metawersum. Warto jednak zadać pytanie: o co w tym wszystkim chodzi?

Konferencja Zuckerberga, który – bez mrugnięcia okiem – opowiedział o podstawowych założeniach platformy rozszerzonej rzeczywistości Metaverse, trwała prawie półtorej godziny. W czasie rzeczywistym śledziło ją natomiast tylko 20 tys. osób. Później żartował z tego polski portal technologiczny Spider's Web. Redaktorzy uznali, że zachwytów brak, bo… nikt na tę technologię nie czekał.

Problemy

Tezę potwierdza Phil Libin, twórca oprogramowania do wideokonferencji Mmhmm. – Podpiąłem gogle VR, ale wytrzymałem tylko kilka minut. Ludzie nie są przystosowani do funkcjonowania z kawałkiem plastiku na twarzy. Zuckerberg próbuje sprzedać pomysł, który już wcześniej się nie przyjął.

Do powyższego rozwiązania chłodno podchodzi też Elon Musk. Założyciel SpaceX i Tesli, a także Człowiek Roku 2021 według magazynu TIME, twierdzi, że idea metawersum (oraz nowoczesnego internetu Web 3.0) go nie przekonuje. – Nie zaprzątam sobie tym głowy – konkluduje Musk.

Czym jest metawersum? To technologia mająca na celu zapewnienie ludziom miejsca do rozmów, korzystania z wirtualnej rozrywki, prowadzenia spotkań czy konferencji, a także po prostu BYCIA. Spełnienie marzeń pisarzy SF oraz technologicznych geeków. Alternatywna rzeczywistość i przestrzeń do prowadzenia drugiego, cyfrowego życia. Może w mniej inwazyjnej formie niż dystopijna przyszłość w filmie „Surogaci" z Bruce'em Willisem – bez szeregu strzelanin i pościgów – ale z mocną ingerencją w dotychczasowy styl życia i przyzwyczajenia ludzi.

Chociaż koncept ten nie jest niczym nowym, to do tej pory pomysł funkcjonował na obrzeżach zainteresowania opinii publicznej. Wygląda na to, że w przyszłości istnieć będzie szereg równoległych metawersów, które mogą – ale nie muszą – wzajemnie na siebie oddziaływać. To, w jakim stopniu użytkownicy będą mogli się ze sobą kontaktować, jest jeszcze niewiadomą.

Korzyści

Entuzjaści przekonują o końcu dotychczasowej formy internetu. Ich zdaniem już wkrótce wszyscy będziemy korzystać z cyfrowego świata metawersum. Pole do popisu jest spore, gdyż funkcjonalność ograniczona jest wyłącznie

ludzką kreatywnością. Przykład? Nissan prowadzi prace nad możliwością pojawienia się jako wirtualny awatar w samochodzie znajomego. W ten sposób można będzie udzielić mu rad lub po prostu towarzyszyć podczas długiej podróży. Największą zaletą innowacji może być zatem eliminacja samotności.

Warto już teraz zadbać o prywatność użytkowników i ich bezpieczeństwo. Będzie wymagało to szeregu uregulowań prawnych – przepisy muszą nadążyć za zmieniającym się światem – a także nabycia nowych, niezbędnych kompetencji cyfrowych.

Zaznaczę ponadto rozwijający się aspekt ekonomiczny. To doskonały czas na inwestycje w tę technologię. Kolejne przedsiębiorstwa tworzące rozwiązania VR pojawiają się codziennie, a ich akcje osiągają zawrotne ceny. Szaleństwo dzieje się też po drugiej stronie ekranu. Wirtualna nieruchomość w cyfrowym świecie Decentraland została sprzedana za 618 tys. kryptowaluty MANA, co dla sprzedającego przełożyło się na zysk 2,4 mln USD!

Sukcesy notuje się również w Polsce. Mateusz Urantówka, założyciel Targów Metaverse oraz start-upu MFA Filming Studio, już kojarzony jest jako przedstawiciel pokolenia metawersum. Zdaniem przedsiębiorcy lata 2024-2025 będą należały właśnie do tej technologii. – W Polsce to prawie nieznany temat. Obudzono ciekawość właścicieli firm IT, ale konsument jeszcze nie zna większości zalet. To się jednak wkrótce zmieni – dodaje Urantówka.

Namiastkę metawersum poznali mali i średni operatorzy telekomunikacyjni. Platforma Avatarland została wykorzystana przy okazji Wirtualnego Kongresu Przedsiębiorców Telekomunikacyjnych. Użycie wirtualnych awatarów umożliwiło w czasach pandemii częściowe oddanie wrażeń płynących z uczestnictwa w wydarzeniu. Miałem okazję przetestować to rozwiązanie i chociaż przypominało bardziej grę z gatunku MMORPG, to nie sposób nie docenić innowacji. Zwłaszcza że normalny kontakt był wtedy niemożliwy.

Czy Zuckerberg przestrzelił?

Prace nad Metaverse przypadły na trudniejszy dla Marka Zuckerberga czas. W ostatnim kwartale ubiegłego roku Facebook stracił ok. pół miliona użytkowników (to pierwszy raz, gdy bilans nowych i usuniętych kont wyszedł negatywny), a 4 lutego 2022 roku cena akcji na giełdzie spadła o 26,39 proc. Wartość Meta Platforms zmalała o 260 miliardów USD, a więc o ¼ wartości spółki. Postawienie na rozwój nowej funkcjonalności, podczas gdy portal społecznościowy przeżywa kryzys, to ryzykowny strzał.

Metawersum będzie jednym z najważniejszych trendów w nadchodzących latach. Jestem jednak przekonany, że nawet najlepiej zrealizowana wirtualna rzeczywistość nie odda złożoności ludzkich relacji społecznych i biznesowych. Czas pokaże, czy gogle VR po jakimś czasie nie wylądują na strychu, obok innych gadżetów. ■

Metawersum będzie jednym z najważniejszych trendów w nadchodzących latach. Jestem jednak przekonany, że nawet najlepiej zrealizowana wirtualna rzeczywistość nie odda złożoności ludzkich relacji społecznych i biznesowych.

MiŚOT DLA UKRAINY

MAREK NOWAK, MICHAŁ KOCH

Przedstawiciele MiŚOT włączyli się w pomoc obywatelom Ukrainy. Transport kilku serwerów, a także innych urządzeń telekomunikacyjnych, został przekazany ukraińskim małym i średnim operatorom przez wolontariuszy Grupy MiŚOT. Podmioty Grupy koordynują także zbiórkę środków dla potrzebujących oraz pomoc w sprawach urzędowych.

– Skontaktowaliśmy się z przedstawicielami INAU, stowarzyszenia zrzeszającego małych ukraińskich operatorów telekomunikacyjnych, i zapytaliśmy ich o bieżące potrzeby – mówi Sebastian Kachel, wiceprezes Stowarzyszenia e-Południe i MiŚOT SA. – Zwrócili się do nas z prośbą o przekazywanie sprzętu sieciowego i IT. By usprawnić pracę, stworzyliśmy w chmurze plik, w którym wpisują konkretne potrzeby, a nasi operatorzy deklarują, co mogą udostępnić.

Zebrany sprzęt został następnie dowieziony na przejście graniczne w Medyce i przeniesiony na stronę ukraińską.

– Organizacja działań pomocowych po polskiej stronie granicy robi duże wrażenie – mówi Marcin Orocz, koordynator transportu Grupy MiŚOT w ramach akcji pomocy Ukrainie. – Niestety trudno było dojechać samochodem pod samo przejście, zdecydowałem się też nie przejeżdżać samochodem, by nie stać w długiej kolejce powrotnej. W efekcie po prostu kilka razy biegałem z serwerami pod pachą.

Przekazany sprzęt trafił bezpośrednio w ręce przedstawicieli ukraińskich ISP z Drohobycza i choć stanowi zaledwie kroplę w morzu potrzeb, szybko przydzielono go do konkretnych zadań. MiŚOT-y zbierają zaś kolejną partię sprzętu za pośrednictwem ISP Forum.

– Bardzo dziękujemy za pomoc! – mówi związany z INUA Aleksandr Tomaszenko. – Z pewnością skorzystamy z tego sprzętu. Najbardziej potrzebujemy teraz serwerów z silnymi procesorami i mocną pamięcią RAM.

Efekty przyniosła także zbiórka MiŚOT dla Ukrainy będąca częścią większej akcji pod szyldem Fundacji Siepomaga. 25 tys. PLN trafiło do

dzieci z domów dziecka spod Lwowa, które od lutego mieszkają w Janowie Podlaskim. Dzięki temu możliwy był zakup niezbędnych do nauki laptopów, drukarek oraz nakładek na klawiatury.

Do Polski przyjeżdżają kolejne dzieci z Buczy, Mariupola i Charkowa. To tereny, gdzie toczą się walki. Nowi goście Zamku w Janowie Podlaskim nie mają praktycznie nic ze sobą. Jeśli ktoś chce pomóc, prosimy o kontakt z Marcinem Oroczem (marcin.orocz@misot.pl).

Grupa MiŚOT otrzymała też specjalne podziękowania od Tarasa Kuczmy, burmistrza Drohobycza.


ДРОГОБИЦЬКА МІСЬКА РАДА

Sebastian Kachel,
Grupa MiŚOT

Taras Kuczma

Burmistrz Drohobycza

LOKALNI dla Uchodźców

W ramach akcji Internet od LOKALNI dla Uchodźców z Ukrainy przygotowane zostały uproszczone dokumenty, takie jak umowa, regulamin oraz niezbędne załączniki przetłumaczone na język ukraiński na bazie wzorców umów telekomunikacyjnych Krajowej Izby Komunikacji Ethernetowej.

– U naszych sąsiadów trwa wojna, a my staramy się im pomagać – mówi Daniel Piecuch z Fundacji Lokalni. – Gościmy w Polsce uchodźców, wspieramy pomoc humanitarną, która trafia za naszą wschodnią granicę. Część MiŚOT-ów wystąpiło także z inicjatywą wspierania uchodźców z Ukrainy poprzez świadczenie im dostępu do internetu na preferencyjnych warunkach. Przygotowaliśmy i udostępniliśmy dokumenty, które mają ułatwić dopełnienie niezbędnych formalności.

Dokumenty dostępne są (nieodpłatnie) w sklepie MiŚOT.

– Dla operatorów głównym miejscem informacyjnym o akcji MdU Internet od LOKALNI dla Uchodźców z Ukrainy jest strona MiWiedza – dodaje Łukasz Biernacki. – Znajdują się tam warunki korzystania, regulamin, a także link do miejsca, z którego można bezpłatnie pobrać dokumenty. Na MiWiedzy znajduje się także sukcesywnie uzupełniane FAQ. Wymiana informacji i doświadczeń trwa także na ISP Forum.

Przy opracowywaniu dokumentów współpracowały: Stowarzyszenie e-Południe, Fundacja Lokalni, Krajowa Izba Komunikacji Ethernetowej, Fundacja Nasza Wizja oraz Kancelaria itB Legal.

– Umowa zawiera niezbędne minimum, powstała na bazie wzorców KIKE i jest zgodna z wymogami UOKiK – podkreśla Ewelina Grabiec z kancelarii itB Legal. – Ponieważ umowa przygotowana jest w dwóch wersjach językowych, a żaden język nie pokrywa się w pełni z innym, należy mieć na uwadze, że zakres znaczeniowy poszczególnych słów może się nieco różnić. Zastosowaliśmy w związku z tym klauzulę „wyboru języka", która stanowi, że w razie wątpliwości rozstrzygająca jest umowa w języku polskim.

Pakiet dokumentów ma jednak na celu jedynie ułatwienie świadczenia uchodźcom usług telekomunikacyjnych na preferencyjnych warunkach.

– Wprowadziliśmy już w naszej firmie usługę nieodpłatnego korzystania z internetu w mieszkaniach udostępnianych uchodźcom – mówi Kamil Kurek, prezes zarządu K3 Telecom. – W praktyce łatwiej było jednak fizycznie zrobić przyłącze niż przygotować dokumenty w języku ukraińskim. Liczymy się z tym, że przez parę miesięcy będzie to usługa świadczona bezpłatnie, a później skończą się działania wojenne lub nasi goście staną na nogi. Do każdego przypadku podchodzić będziemy indywidualnie – zaznacza.

Pomoc trwa

– Kontynuujemy wspieranie działającego w Drohobyczu stowarzyszenia zrzeszającego małych ukraińskich operatorów telekomunikacyjnych INAU – mówi Marcin Orocz. – Ze strony ukraińskiej zbieraliśmy informacje o bieżących potrzebach, a związani z Grupą MiŚOT lokalni operatorzy deklarowali, jaki sprzęt mogą przekazać. Wszystko odbywało się za pomocą formularza w serwisie Google.

Sprzęt został przekazany przez firmy Syrion, Systel i MCI Tychy, zaś transport przebiegł sprawnie, choć nie zabrakło też niespodzianek. Jedną z nich była niesłychanie długa kolejka na przejście granicznie w Medyce w stronę Ukrainy. Jest to związane ze zniesieniem ceł na samochody używane.

– Po kontakcie z przedstawicielami ukraińskich ISP na miejsce spotkania wybraliśmy ostatecznie przejście Budomierz–Hruszew – relacjonuje Marcin Orocz.

Rozproszone i często pokrywające się sieci małych i średnich operatorów w Ukrainie okazały się w warunkach wojny trudniejsze do zniszczenia. W utrzymaniu łączności bardzo pomaga też sieć Starlink, są jednak rejony, które wymagają wsparcia. Pomoc ze strony Grupy MiŚOT będzie kontynuowana. ■

IDEE SĄ KULOODPORNE

Historia Anonymous

MICHAŁ KOCH

Atak Rosji na Ukrainę odbił się szerokim echem w świecie cyfrowym. Grupa hakerska Anonymous opowiedziała się po stronie broniących kraju Ukraińców i zobowiązała do nękania Rosjan w cyberprzestrzeni. Kim zatem są ci zamaskowani aktywiści?

Przenieśmy się na chwilę do 1605 roku. W Anglii konspiratorzy planują tzw. spisek prochowy. Ich celem jest Jakub I, król Anglii i Szkocji. Jeden z zamachowców, Guy Fawkes, zostaje złapany, torturowany i stracony. Rewolta się nie udaje, ale postać Fawkesa nabiera symbolicznego wymiaru. Tworzy się legenda bojownika. Jego znakiem rozpoznawczym staje się charakterystyczna maska.

W 2006 roku na scenę wkraczają Anonymous. Zaczynają skromnie – od sieciowego wandalizmu, wykradania kodów źródłowych programów i drobnych ataków hakerskich. Powoli wykuwają własny mit, tworzą cyfrowy kodeks moralny. Wkrótce angażują się w sprawy państw Bliskiego Wschodu, wspierają Arabską Wiosnę i zaczepiają tamtejsze reżimy. Przyrzekają zwalczać faszyzm, ale stają również w obronie wolności w internecie. Są wśród niezadowolonych, gdy światowe rządy próbują wprowadzić porozumienie ACTA (Anti-Counterfeiting Trade Agreement). Ich działania nabierają rozgłosu, użytkownicy sieci szybko zaczynają identyfikować się z prezentowanymi wartościami. Powstaje hacktivism, a ruch zaczyna być kojarzony z maską Fawkesa.

Obecnie Anonymous bacznie śledzą wszystkie wydarzenia na planecie. Ze światem komunikują się poprzez Twittera, krótkie filmiki imitujące programy informacyjne i branżowe fora. Zgodnie z ich sloganem „we are legion" – każdy może być jednym z nich.

Nie dziwi więc, że rosyjska inwazja ich zdenerwowała. Putin i jego przyboczni dopuścili się bezczelnych kłamstw, zastosowali cenzurę w mediach i zaatakowali ludność cywilną. Wkroczyli więc Anonymous. Przestrzegli, że będą gnębić Rosję w sieci, wypowiedzieli mocarstwu cyberwojnę. Począwszy od ataków na strony rosyjskich organów państwowych aż po wykradanie informacji operacyjnych i niewielkie akty złośliwości, takie jak np. zmiana znaku wywoławczego jachtu rosyjskiego prezydenta na „fckptn". Do Putina zwrócili się bezpośrednio. Poinformowali, że znają jego tajemnice i wkrótce je upublicznią. Nawet jeśli to blef, to i tak musiało zaboleć. Wszyscy podejrzewamy przecież, że Kreml ma sporo mrocznych sekretów.

Czy Anonymous naprawdę mają informacje dotyczące rosyjskich agentów rezydujących w krajach Zachodu? Hakerzy twierdzą, że po ich upublicznieniu w wielu państwach dojdzie do trzęsienia ziemi. Wszak lista podmiotów z Rosji, których zabezpieczenia już złamali, jest imponująca. W sieci już krąży ogromny zbiór danych, które wyciekły z rosyjskiego ministerstwa obrony, a agencja kosmiczna Roskosmos przekazała, że hakerzy wyłączyli centrum kontroli lotów.

Haktywiści ostrzegają też przed naciągaczami. Ich kodeks moralny zakłada brak zysków finansowych. Nie hakują dla pieniędzy, hakują dla idei. Ta forma stawiania oporu ma jednak także przeciwników. Specjaliści zajmujący się cyberbezpieczeństwem przestrzegają. Zdaniem wielu włamania sieciowe, nawet w dobrej sprawie, są przejawem wandalizmu i mogą być niebezpieczne.

Sądzę, że Anonymous na stałe wpisali się w krajobraz sieci. Jest o nich coraz głośniej, kibicują im zwykli ludzie, którzy chcieliby zakończyć wojnę na Ukrainie bez rozlewu krwi, upokarzając przy okazji Putina. Wydaje się też, że i sami Anonymous nie są skorzy do odpuszczenia grzechów Rosji bez względu na koszty. Wszystko zgodnie z hasłem „idee są kuloodporne", które wypowiada V, skrywający się za maską Guya Fawkesa, anarchista, bojownik o wolność oraz bohater komiksu i filmu „V jak Vendetta". ■

BRIGHTSPOT
LAW | AUDIT | CONSULTING

BRIGHTSPOT CONSULTING

Usługodawca:
Brightspot Consulting

ul. Zwierzyniecka 17/3
31-103 Kraków

tel. 12 311 04 42
biuro@brightspot.pl
www.brightspot.pl

Opis:

Brightspot Consulting jest wyspecjalizowaną firmą doradczą świadczącą usługi dla podmiotów z branży telekomunikacyjnej.

Do naszych usług należy:

- Sporządzanie raportów ryzyk prawnych i podatkowych na potrzeby wewnętrzne (między innymi weryfikacja wzorców dokumentacji abonenckiej, analiza umów z kontrahentami, relacje z właścicielami nieruchomości, problem OZZ, ocena efektywności przyjętej struktury korporacyjnej, optymalizacje w zakresie podatku od nieruchomości);
- Sporządzanie wycen sieci oraz przedsiębiorstw telekomunikacyjnych;
- Audyt prawny i podatkowy na potrzeby uzyskania finansowania bankowego oraz na potrzeby zakupu lub sprzedaży firmy;
- Pozyskiwanie finansowania na inwestycje (rozbudowa infrastruktury) oraz akwizycje (zakup komplementarnych sieci oraz konkurencyjnych przedsiębiorstw);
- Kompleksowa obsługa transakcji sprzedaży sieci, na którą składają się wycena sieci, audyt wewnętrzny, określenie modelu sprzedaży pod kątem organizacyjnym i podatkowym, pozyskanie nabywcy, negocjacje ceny i warunków transakcji, sporządzenie umowy i finalizacja transakcji.

Aby zapoznać się z pełnym zakresem naszych usług zachęcamy do kontaktu oraz odwiedzenia strony internetowej www.brightspot.pl.

Zapraszamy do współpracy.

MiSOT GRUPA

MiSOT S.A.

EPIX MiSOT

EPIX jest największym w Polsce niekomercyjnym, prawdziwie neutralnym i niezależnym węzłem wymiany ruchu IP. Zarządzany przez operatorów ISP, działa na zasadzie not for profit – nadwyżki finansowe pozyskane z jego prowadzenia przeznaczane są na przedsięwzięcia służące jego użytkownikom. Współpraca bazuje na wzajemnym zaufaniu i zadowoleniu. EPIX zapewnia operatorom tani i prosty dostęp do treści pozostałych polskich IX-ów oraz wszystkich integratorów IPTV. Podłączenie do węzłów EPIX jest możliwe w jednej z trzech kolokacji – w Katowicach, w Warszawie lub w Poznaniu.

MdM MiSOT

MdM, czyli Media dla MiŚOT, prowadzi najważniejsze media w środowisku. Lokalni operatorzy mogą z nich czerpać wiedzę i bieżące informacje. Wśród kanałów komunikacji zarządzanych przez spółkę znajdują się: najpopularniejsze forum polskich operatorów telekomunikacyjnych – ISP Forum, jedyny magazyn branży ICT (kwartalnik drukowany i dostępny on-line) – ICT Professional, cotygodniowy newsletter skierowany do lokalnych dostawców usług – MiŚOT PING oraz opiniotwórczy portal z najświeższymi informacjami ze świata, kraju i lokalnych rynków – ISPortal. Media MdM są ogromną bazą wiedzy o telekomunikacji, prawie, trendach i biznesie zebraną w formie newsów, felietonów, analiz, porad i wywiadów.

MdO MiSOT

Projekt MdO, czyli Mały i Średni Operator Telekomunikacyjny dla Ogólnopolskich (przetargów, konkursów, klientów), umożliwił MiŚOT-om start pod wspólną marką w przetargach na budowę Ogólnopolskiej Sieci Edukacyjnej. Dzięki temu wyrównano szanse w stosunku do operatorów korporacyjnych, a mniejsi operatorzy odnieśli sukces – pozyskali w latach 2018 – 2021 w postępowaniach organizowanych przez NASK ponad 3000 lokalizacji. W Projekcie MdO uczestniczy kilkuset MiŚOT-ów. Dzięki udziałowii w przedsięwzięciu, zarobili oni w 2021 roku prawie 10 mln zł, a szacowane przychody do 2025 roku przekroczą 45 mln zł.

PROJEKTY

MiSOT Projekt TeleCentrum

TeleCentrum to profesjonalne call center dopasowane do potrzeb i możliwości finansowych MiŚOT. Projekt ten wspiera operatorów z całej Polski, odciążając pracę biura i zastępując je poza standardowymi godzinami pracy. Działa w trybie całodobowym siedem dni w tygodniu. TeleCentrum zostało szczególnie docenione przez lokalnych operatorów w czasie pandemii. Usługa zdalnego call center pomogła wielu przedsiębiorcom telekomunikacyjnym opanować zaistniałe zakłócenia w swoich procesach biznesowych.

MiSOT Projekt TeleKlasa

TeleKlasa to platforma wspierająca zdalną edukację, a zarazem wkład Fundacji Lokalni i Stowarzyszenia e-Południe w tworzenie pro publico bono systemowych rozwiązań opartych o infrastrukturę MiŚOT-ów. TeleKlasa korzysta z oprogramowania open source oraz autorskiego systemu zarządzania serwerami. Platformę wspierają również lokalne firmy zaangażowane w projekt – Anioły Mocy Obliczeniowej (AMO). Współpracując z klastrem e-Południe również możesz zostać AMO i oferować to zaawansowane rozwiązanie w swoich lokalnych społecznościach. Pomyśl, jak w Twojej miejscowości prowadzone jest zdalne nauczanie? Czy w pełni oferujesz lokalnie rozwiązania, do których masz dostęp?

MiSOT Projekt TeleOdpowiedzialni

Inicjatywa TeleOdpowiedzialni promuje w środowisku Małych i Średnich Operatorów Telekomunikacyjnych społeczną odpowiedzialność biznesu. Dzielimy się wiedzą, dyskutujemy o modelach współpracy z regionalnymi mediami, wspieramy innowacyjność i wzmacnianie relacji z lokalną społecznością, promujemy ograniczanie negatywnego wpływu działalności przedsiębiorstw na środowisko. Stowarzyszenie e-Południe stworzyło w 2018 roku pierwszy w branży telekomunikacyjnej kodeks, w oparciu o który w obszarze społecznej odpowiedzialności biznesu działają MiŚOT-y. Kluczowym przedsięwzięciem w projekcie jest konkurs TeleOdpowiedzialny Roku, w którym kapituła wyróżnia MiŚOT-ów z całej Polski mogących pochwalić się kompleksowym podejściem do społecznej odpowiedzialności biznesu lub ciekawymi inicjatywami CSR-owymi. Jednym z priorytetów dla Grupy MiŚOT na najbliższe lata jest dalsza promocja CSR wśród małych i średnich operatorów telekomunikacyjnych.

e-POŁUDNIE STOWARZYSZENIE

MdS MiSOT

Spółka powstała w celu wypracowania rozwiązań i produktów podnoszących poziom cyberbezpieczeństwa. Podmiot pracuje nad rozwiązaniem zabezpieczającym segmenty sieci administrowane przez ISP przed całym spektrum anomalii ruchu sieciowego. Obecnie przedsięwzięcie przechodzi od etapu projektowego do etapu budowy prototypu plaformy testowej.

MdI MiSOT

MiŚOT dla internetrzeczy.pl. Spółka, której celem jest wykorzystanie potencjału związanego z rozproszonym położeniem w kraju MiŚOT-ów, ich możliwości technicznych, biznesowych do budowy i utrzymania ogólnopolskiej sieci LoRaWAN. Popularyzacja tej technologii pozwoli na oferowanie nowych produktów, związanych z monitorowaniem procesów gospodarczych, infrastrukturalnych oraz zapewniających bezpieczeństwo funkcjonowania firm, instytucji i społeczności lokalnych.

FUNDACJA LOKALNI

Fundacja Lokalni i inicjatywa TeleOdpowiedzialni promują w środowisku Małych i Średnich Operatorów Telekomunikacyjnych społeczną odpowiedzialność biznesu. Dzielimy się wiedzą, dyskutujemy o modelach współpracy z regionalnymi mediami, wspieramy innowacyjność i wzmacnianie relacji z lokalną społecznością. Promujemy ograniczanie negatywnego wpływu działalności przedsiębiorstw na środowisko.

LOKALNI.PL

Projekt Lokalni zakłada zwiększenie przychodów uczestników, jak i oszczędność czasu i pieniędzy. Jego celem jest promowanie marek w ramach idei lokalności: na stronie www.lokalni.pl oraz na facebooku: www.facebook.com/LOKALNIsaPROFESJONALNI.

W ramach projektu prowadzone są , na szeroką skalę, działania marketingowe: od promocji w internecie, przez produkcję materiałów reklamowych i promocyjnych, aż po reklamę w mediach ogólnopolskich. Projekt promuje marki rozpoznawalne na lokalnym rynku. Ułatwia to wspólną wyszukiwarką usług telekomunikacyjnych: www.lokalni.pl, którą wypełniono zasięgami, a także działaniami w social marketingu. Jako bonus w projekcie uczestnicy otrzymują pakiet form graficznych do wykorzystania, aby ich profile w mediach społecznościowych były stale aktualizowane.

Rok 2020 był dla przedsięwzięcia fazą startupową. Był to czas budowania społeczności na Facebooku, gdzie wygenerowano ponad 10 tys. reakcji fanów i ponad 1,7 mln wyświetleń postów i filmów.

JAK DOŁĄCZYĆ

1. Jeśli jeszcze tego nie zrobiłeś, najpierw wejdź i zarejestruj się na stronie https://www.epix.net.pl/rejestracja/ i odbierz swój EPID. Rejestracja jest bezpłatna. Dzięki temu uzyskasz dostęp do wielu kanałów informacji i od razu będziesz mógł brać czynny udział w projektach nie wymagających żadnych opłat.
2. Śledź na bieżąco informacje w ogólnodostępnych mediach dla MiŚOT. Zaprenumeruj cotygodniowy newsletter MiŚOT PING oraz branżowy kwartalnik ICT Professional. Załóż konto na ISP Forum i zapisz się do grupy #drMiŚOT.
3. Bierz aktywny udział w darmowych obecnie projektach klastrowych, np. TeleKlasa lub lokalni.pl.
4. Wreszcie zainteresuj się komercyjnymi projektami klastra (EPIX, TeleCentrum), dzięki którym Twój biznes operatorski zyska jeszcze większego przyspieszenia.

Jeśli jednak wolisz porozmawiać, zawsze możesz do nas zadzwonić:

+48 -780-118-730

Paweł Białas / dyr. ds. rozwoju

LOKALNE ZJAZDY MiŚOT

misot.pl/zjazdy

MiSOT GRUPA

Krajowa Izba Komunikacji KIKE Ethernetowej

nasza wizja

gdzieś na zachodzie

Kołobrzeg

Janów Podlaski

Bukowina Tatrzańska