ISPROFESSIONAL

ISSN: 2449-5581

#6 (KWIECIEŃ 2024)

PROJEKT MdS
wdraża wymagania dyrektyw NIS2 u operatorów

WWW.EPIX.NET.PL

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

Jesteśmy największym IXP w Polsce, opartym na trzech niezależnych węzłach: Katowice, Warszawa i Poznań. Powstaliśmy, aby dbać o interesy i zaspokajać potrzeby polskich MiSOT-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. Natomiast Projekt TeleSynergia zainicjowaliśmy we współpracy z Beyond.pl, dostawcą zielonych i najbezpieczniejszych usług data center i cloud w Europie, umożliwiając dostęp kolejnym operatorom międzynarodowym do EPIX oraz poprawiając bezpieczeństwo przesyłu danych. Korzystają na tym nasi klienci.

800+ UCZESTNIKÓW

3.0 Tb/s+ RUCHU IP

1300+ PORTÓW

MiSOT GRUPA

OD REDAKCJI

AUTOR
Redakcja

Drodzy Czytelnicy,

W dzisiejszych czasach, kiedy rynek telekomunikacyjny ewoluuje z niespotykaną dotąd szybkością, dostosowanie się do zmieniającej się rzeczywistości i wykorzystanie nowych technologii staje się nie tylko możliwością, ale przede wszystkim koniecznością. Właśnie w tym kontekście grupa MiŚOT odgrywa kluczową rolę, demonstrując zdolność do innowacji, co pozwala na efektywne konkurowanie nawet z dużymi graczami na rynku.

W tym wydaniu skupiamy się na szeregu tematów, które są obecnie na ustach wszystkich w branży: od najnowszych trendów w technologiach sieciowych, przez cyfrową transformację, po strategie rozwoju i zarządzanie w sektorze MiŚOT. Chcemy, aby ISProfessional służył nie tylko jako źródło cennych informacji, ale również jako platforma wymiany doświadczeń i najlepszych praktyk, która inspiruje do poszukiwania nowych, kreatywnych rozwiązań.

W tym numerze znajdziecie również relacje z ostatnich wydarzeń branżowych, wywiady z liderami opinii oraz analizy przypadków, które mam nadzieję, staną się dla Was źródłem inspiracji i motywacji do dalszego rozwoju.

Życzymy przyjemnej lektury!
Redakcja ISProfessional

Projekt ISProfessional #6 (kwiecień 2024) wydany w kwietniu 2024 r. realizowany jest pod patronatem Grupy MiŚOT.
Redakcja i wydawca nie ponoszą odpowiedzialności za publikowane treści. Prezentowane poglądy i opinie są opiniami danej osoby i redakcja w żaden sposób nie utożsamia się z nimi

~~~~~~

Administratorem Państwa danych jest **Projekt MdM** Spółka z ograniczoną odpowiedzialnością z siedzibą w Bytomiu, ul. Antoniego Józefczaka 29/40, 41–902 Bytom, wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy Katowice-Wschód w Katowicach pod numerem KRS: 0000765400, NIP: 6263032549, REGON: 382090808, kapitał zakładowy w kwocie 500.000,00 złotych, zwaną dalej: „MdM", reprezentowaną przez Pana Krzysztofa Fujarskiego – Prezesa Zarządu.

Informacje na Państwa temat posiadamy z publicznie dostępnego źródła – Rejestru przedsiębiorców telekomunikacyjnych. Dane, jakie posiadamy i przetwarzamy to imię, nazwisko, nazwa firmy, adres firmy, NIP, KRS, adres e-mail. Mają Państwo możliwość zażądania, aby nie otrzymywać więcej takich informacji.

Określone powyżej informacje na Państwa temat posiadamy po to, by wysyłać Państwu magazyn ICT Professional o produktach, usługach, innowacjach oraz aktualnościach, jakie naszym zdaniem mogą być dla Państwa interesujące.

Dostęp do danych będą miały osoby pracujące i współpracujące z nami w zakresie realizacji na Państwa rzecz usług. Informacje na Państwa temat nie będą przekazywane poza terytorium Unii Europejskiej.

Pragniemy wysyłać Państwu informacje o produktach, usługach, innowacjach oraz aktualnościach, które mogą być dla Państwa interesujące. Mają Państwo prawo, by w dowolnym czasie zażyczyć sobie, abyśmy zaprzestali kontaktowania się z Państwem w celach marketingowych.

Państwa dane osobowe przetwarzane są w celach marketingowych związanych z przesyłaniem Państwu magazynu, będziemy przechowywać do chwili otrzymania od Państwa żądania zaprzestania kontaktowania się ww. celu. Mają Państwo prawo zażądać kopii informacji przechowanych przez nas na Wasz temat. Chcemy zapewnić, aby Państwa dane osobowe były zawsze prawidłowe i aktualne, zatem jeśli zauważą Państwo nieprawidłowości, możecie Państwo zwrócić się do nas o skorygowanie lub usunięcie informacji, które uznacie za nieprawidłowe lub nieścisłe. Mogą Państwo także złożyć skargę w Urzędzie Ochrony Danych Osobowych pod adresem ul. Stawki 2, 00–193 Warszawa.

Kontakt z redakcją:
prasa@misot.pl

Nr w rejestrze wydawnictw:
PR2614

Międzynarodowy znak informacyjny:
ISSN 2449-5581

Redaktor naczelny:
Krzysztof Fujarski

Sekretarz redakcji:
Michał Koch
michal.koch@misot.pl

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

Redakcja:
Paweł Gniadek
Marek Nowak
Klaudia Wojciechowska

Projekt graficzny, skład i grafika na okładce:
Justyna Kramarz [goodot.pl]

Wybrane grafiki – Marcin Jedynak, freepik.com, pixabay.com

Wydawca:
Projekt MdM Sp. z o.o.
ul. Józefczaka 29/40
41–902 Bytom

Przedruk i kopiowanie tylko za zgodą redakcji

Korekta:
Małgorzata Kościcka

Współpraca:

Paweł Białas
Łukasz Biernacki
Aleksandra Czerech
Krzysztof Czuszek
Michał Filipek
Sebastian Kachel
Adam Kossowski
Maciej Linscheid
Marcin Pilak
Wojciech Szymczak
Anna Walter
Piotr Wasyk
Krzysztof Zawadzki
Marcin Zemła
~~~~~~

Spis treści

Produkty marki cudy

w XBEST.pl
fibre optic cables & accessories

Nowoczesne rozwiązania sieciowe dla domu i biura

Technologia
Wi-Fi6

WHOLE HOME
MESH

Transmisja
2.5Gbps

Superszybkie Wi-Fi
AX3000

Tryb CCTV/VLAN
zasięg do 250m

Do 30W
na port PoE+

xbest.pl Sp. z o.o. | **Siedziba:** 00-807 Warszawa, Al. Jerozolimskie 96 **Oddział w Rybniku:** 44-200 Rybnik, Św. Józefa 141D
+48 32 239 60 00 i 01, fax.: +48 32 239 6010 office@xbest.pl www.xbest.pl

AUTOR
Marek Nowak

Projekt MdS wdraża
wymagania dyrektyw NIS2 u operatorów

Potrzeba wdrożenia dyrektywy NIS2, czyli w praktyce zrewolucjonizowania podejścia do cyberbezpieczestwa, powoli toruje sobie drogę w środowisku małych i średnich operatorów telekomunikacyjnych. Eksperci są zgodni, że nie warto już czekać i trzeba liczyć się z wydatkami.

Państwa członkowskie Unii Europejskiej wdrożyły już pierwszą dyrektywę NIS (Network and Information Security), zrobiły to jednak w różnorodny sposób. Doprowadziło to do fragmentacji rynku wewnętrznego w zakresie jego cyberodporności. Pojawiły się też nowe cyberzagrożenia. W związku z powstałą potrzebą zwiększenia i ujednolicenia cyberodporności wszystkich państw członkowskich, przepisy unijne zostały zaktualizowane dyrektywą NIS2.

Dyrektywa ta wprowadza szczegółowe regulacje dotyczące infrastruktury krytycznej i weszła już w życie. Wszystkie państwa członkowskie są zobowiązane do jej wdrożenia do 17 października 2024 roku. Choć w Polsce czekamy jeszcze na projekt odpowiedniej ustawy, właściwie wiemy jakie wymagania postawi przed przedsiębiorcami. Będą też z pewnością zbieżne z wytycznymi ENISA w zakresie cyberbezpieczeństwa sieci i usług komunikacji elektronicznej. Nie ma wątpliwości, że nowe regulacje obejmą przedsiębiorców telekomunikacyjnych.

Szykuj się!

– W ramach przygotowań operatorów telekomunikacyjnych do wejścia w życie dyrektywy NIS2, Projekt MdS Sp. z o.o. zakończył w ostatnim czasie wdrożenia elementów Systemu Zarządzania Bezpieczeństwem Informacji w kilku podmiotach i szykuje się do rozpoczęcia kolejnych wdrożeń w drugim kwartale tego roku – mówi Bartosz Smulczyński, członek zarządu spółki. – Pamiętać trzeba, że jedno takie wdrożenie to okres od 2 do 6 miesięcy. Nie warto więc czekać do

ostatniej chwili, bo może się okazać, że trzeba będzie przepłacić albo czekać w kolejce na wykonanie zlecenia – dodaje.

Eksperci są zgodni, że nowe procedury związane z cyberbezpieczeństwem oznaczać będą w praktyce m.in. nowe procedury obsługi incydentów, zapewnienia ciągłości działania i bezpieczeństwo łańcucha dostaw, procesów nabywania, rozwijania i utrzymania systemów informatycznych oraz nowe polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie.

Dyrektywa kładzie też duży nacisk na szkolenia z zakresu cyberbezpieczeństwa, a także stosowanie kryptografii. Warto również pamiętać o nowych terminach zgłaszania do CSIRT ostrzeżeń o wykrytych incydentach (24 godziny) oraz zgłaszania samych incydentów (72 godziny). Terminy są zatem zbliżone do wysokich wymogów określonych w przepisach o ochronie danych osobowych.

Warto też przypomnieć, że nowe regulacje określają również wysokie kary za naruszenia przepisów cyberbezpieczeństwa. W niektórych przypadkach mogą one sięgnąć nawet 10 000 000 euro lub 2% rocznego obrotu.

Jakie to koszty?

Nie jest tajemnicą, że wprowadzenie NIS2 spowoduje wzrost kosztów prowadzenia działalności wielu przedsiębiorców telekomunikacyjnych. Na Zjeździe MiŚOT w Zakopanem mówił o tym między innymi Dariusz Fudala z firmy SayF. Zaznaczył przy tym, że spełnienie tych obowiązków leży także w interesie przedsiębiorców i jest to po prostu potrzebne.

WARTO RÓWNIEŻ PAMIĘTAĆ O NOWYCH TERMINACH ZGŁASZANIA DO CSIRT OSTRZEŻEŃ O WYKRYTYCH INCYDENTACH (24 GODZINY) ORAZ ZGŁASZANIA SAMYCH INCYDENTÓW (72 GODZINY)

Choć szacunki się różnią, według ekspertów w ciągu najbliższych trzech do czterech lat firmy będą musiały zwiększyć swoje wydatki na cyberbezpieczeństwo o około 20-25 proc. Wydatki te mogą być mniejsze w przedsiębiorstwach, które wcześniej wdrożyły wszystkie wymagania NIS i dysponują cyberochroną na poziomie obowiązującej już dyrektywy. Tu szacowany wzrost wydatków ma wynieść około 12-15 proc.

Dodatkowe informacje w zakresie przygotowania przedsiębiorstwa do Dyrektywy NIS2 można uzyskać poprzez kontakt ze spółką Projekt MdS na adres: biuro@projektmds.pl

AUTOR
Marek Nowak

Społeczność smart & safe

Rozbudowa sieci monitoringu miejskiego, czujniki otwarcia i zamknięcia pomieszczeń oraz monitorowanie jakości powietrza to zadania, które lokalni operatorzy telekomunikacyjni oferują dziś gminom w oparciu o platformę Sencito.

Gminy coraz częściej wprowadzają i rozbudowują sieci lokalnego monitoringu. Na potrzebę większej liczby kamer zgodnie zwracają uwagę mieszkańcy, samorządowcy i policja. Zwiększenie liczby kamer może też być argumentem w zbliżającej się kampanii samorządowej. Radni i kandydaci na radnych mogą też proponować, gdzie zainstalować kamery. Oczywiście wszystko powinno odbywać się na podstawie danych policji.

Operatorzy w akcji

Podjąć się tego zadania mogą zaś lokalni operatorzy telekomunikacyjni, dobrze znani mieszkańcom. Przedstawiciele MiŚOT-ów mają do zaoferowania gminom rozwiązania oparte o system Sencito, opracowany przez czeską firmę Master IT. Przy okazji w gminie mogą też pojawić się pewne dodatkowe gadżety, a mianowicie instrumenty monitorujące jakość powietrza w mieście lub czujniki informujące o otwarciu pomieszczeń czy klap studzienek kanalizacyjnych, co także zwiększa bezpieczeństwo mieszkańców, a szczególnie dzieci.

– W rozmowach z przedstawicielami gminy wykorzystaliśmy argument, że podłączenie kamer monitoringu jest możliwe w ramach szerszej platformy – mówi Artur Tomaszczyk z ComNet Multimedia. – Poza kwestiami związanymi stricte z bezpieczeństwem urzędnicy zweryfikują przestrzeganie przepisów drogowych (szybko ograniczone zostanie parkowanie w miejscach do tego nieprzeznaczonych). Zaproponowaliśmy także instalację kilku inteligentnych czujników pogodowych pracujących na bazie sieci LoRaWAN. Pozwolą one rolnikom sprawdzić stan opadów z ostatnich godzin i dni. W wybranych budynkach publicznych monitorowany będzie także poziom dwutlenku węgla.

Gotowe rozwiązanie dedykowane małym i średnim operatorom telekomunikacyjnym dostępne są praktycznie od ręki. Odpowiada za nie Projekt MdI (MiŚOT dla Internetu Rzeczy), który jest częścią Grupy MiŚOT integrującej przedsiębiorców tej branży w skali ogólnopolskiej.

OPERATOR NEGOCJUJE Z GMINĄ WŁASNĄ MARŻĘ, PRZEPROWADZA INSTALACJĘ, A KOLEJNA INGERENCJA W SYSTEM WYMAGANA BĘDZIE OD NIEGO DOPIERO ZA KILKA LAT, GDY NASTĄPI KONIECZNOŚĆ WYMIANY BATERII W CZUJNIKACH

– Lokalni operatorzy mogą już dzisiaj zarabiać na tych rozwiązaniach – dodaje Artur Tomaszczyk.

W ofercie Sklepu MiŚOT dostępne są różnorodne czujniki Sencito (od trackerów GPS po detektory środowiskowe, w tym poziomu wody i hałasu). Jednym z ciekawszych praktycznych zastosowań tej technologii jest też tablica LED, która dokonuje pomiarów prędkości uczestników ruchu drogowego i przekazuje je do systemu. Dzięki temu przedstawiciele administracji wiedzą, kiedy dochodzi do przekraczania prędkości. Następnie dane te mogą być wykorzystywane do tworzenia analiz i symulacji, aby finalnie doprowadzić do zwiększenia bezpieczeństwa na drogach. Innym przykładem są trackery, które można zainstalować np. w szkolnych autobusach.

Społeczności bliżej siebie

Warto dodać, że aplikacja Sencito posiada także wbudowane powiadomienia push, dzięki czemu na urządzeniach końcowych użytkowników mogą pojawiać się informacje, takie jak na przykład: harmonogram odśnieżania gminnych ulic, komunikaty o zaginięciach i odnalezieniach zwierząt domowych czy aktualności ze strony internetowej należącej do gminy. Jest to więc także podstawa budowania smart community i szansa na eliminację wykluczenia cyfrowego.

– Wdrożenie tych rozwiązań jest proste i wymaga jedynie niewielkiego zaangażowania ze strony lokalnych operatorów – podkreśla Wojciech Ogonek z projektu MdI. – Grupa MiŚOT zapewnia operatorom infrastrukturę w postaci bramki i antenę LoRaWAN (należy ją skonfigurować do Ipv6), a także utrzymuje platformę Sencito na swoich serwerach w stałej cenie. Operator negocjuje z gminą własną marżę, przeprowadza instalację, a kolejna ingerencja w system wymagana będzie od niego dopiero za kilka lat, gdy nastąpi konieczność wymiany baterii w czujnikach. Wszystko jest jasne i przejrzyste.

Dzięki ofercie Grupy MiŚOT rozwiązania smart mogą już niebawem na stałe zagościć w mniejszych miejscowościach Polski.

Więcej dowiedzieć się można bezpośrednio w dziale handlowym od Wojciecha Ogonka: e-mail: wojciech.ogonek@misot.pl; tel.: 797 301 309.

AUTOR
Marcin Zemła

Rada Bezpieczeństwa Biznesowego Grupy MiŚOT
zaczęła pracę

Obywatele, rodacy, Rzymianie! Niezwykle miło jest mi poinformować, że po długiej i ciężkiej walce, Rada Bezpieczeństwa Biznesowego Grupy MiŚOT zaczęła swoje prace. Znaleźli się wśród was ludzie, którym leży na sercu nasz rozwój i ochrona przed zagrożeniami, zarówno zewnętrznymi, jak i wewnętrznymi.

Co wam da Rada Bezpieczeństwa?

Do swoich przedstawicieli, regionalnych członków rady, proszę, abyście zgłaszali wszelkie patologie dużych telekomów, które dzieją się w ramach nieuczciwej konkurencji. Za pośrednictwem mejla przesyłamy do członka Rady w regionie opis sytuacji, dowody (pisma, zdjęcia itp.). To materiały na nasze spotkania, podczas których co miesiąc będziemy podejmować decyzje, co z tym zrobić. Prokuratura, Sąd, UOKIK, UKE czy KIKE plus nacisk medialny i piętnowanie takich praktyk.

Jesteście małymi i średnimi operatorami telekomunikacyjnymi. Jesteście wyjątkowi na tle rynku telekomunikacyjnego w Europie. To zobowiązuje. Wszelkie spory możecie rozwiązywać wewnętrznie z udziałem Sądu Koleżeńskiego (kierując sprawę do Rady). Tu ponownie prosimy o opis problemu z innym naszym telekomem i o dowody. Sąd Koleżeński wyda opinię, abyście mieli ocenę obiektywną, która ma przede wszystkim na względzie dobro wspólne, bez robienia sobie krzywdy.

Rekomendacje techniczne

Rada zbiera informacje od EPIXA i MDS, informacje prawne oraz informacje od was samych o podatnościach, sprzęcie, konfiguracjach, łańcuchach dostaw,

obowiązkach prawnych, dostosowaniu się do demonów (sprawozdania, NIS, PIT i inne skróty). Konsultuje następnie ten materiał z ekspertami i buduje rekomendacje. Zbiór tych rekomendacji będzie stanowił Kodeks Dobrych Praktyk Grupy MiŚOT, który przekażemy do ENISA (europejskiej instytucji budującej wytyczne w zakresie cyberbezpieczeństwa).

Kodeks Etyki

Jak już wcześniej pisałem być MiŚOT-em to zaszczyt. Dlatego uważamy, że należy kształtować właściwe zachowania i postawy, żeby duzi zaczęli się wstydzić i zrozumieli, że nie jesteśmy robactwem do wytępienia ani łatwym żerem dla dużych.

A zatem korzystajcie z tego organu, ile fabryka dała. To jest dla was, żeby was skutecznie chronić bez zbędnej polityki.

WSZELKIE SPORY MOŻECIE ROZWIĄZYWAĆ WEWNĘTRZNIE Z UDZIAŁEM SĄDU KOLEŻEŃSKIEGO (KIERUJĄC SPRAWĘ DO RADY). TU PONOWNIE PROSIMY O OPIS PROBLEMU Z INNYM NASZYM TELEKOMEM I O DOWODY

Sąd Koleżeński wyda opinię, abyście mieli ocenę obiektywną, która ma przede wszystkim na względzie dobro wspólne, bez robienia sobie krzywdy.

Z ŻYCIA MIŚOT

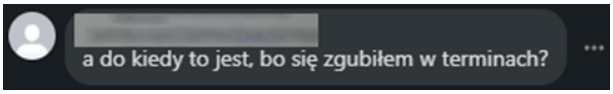
AUTOR
Michał Koch

Krajobraz po PITwie

Gdy po raz pierwszy usłyszałem, że na operatorów nałożono obowiązki związane z raportowaniem SIDUSIS oraz PIT podskórnie czułem, że zwiastuje to kłopoty. Czy branży telekomunikacyjnej udało się wypracować rozwiązanie dotyczące powyższego obowiązku w sposób akceptowalny dla wszystkich stron?

Urząd Komunikacji Elektronicznej przypomina o konieczności przekazania danych w ramach inwentaryzacji infrastruktury i usług telekomunikacyjnych. Operatorzy powinni poznać terminy, w których mają obowiązek raportować dane do Punktu Informacyjnego ds. Telekomunikacji (PIT).

Powyższy komunikat UKE zapewne wielu zmroził lub wprawił we wrzenie. Polscy operatorzy znowu coś muszą. Znowu dokłada się im pracy. Warto w tym miejscu przypomnieć, że telekomunikacja to strategiczna dziedzina funkcjonowania kraju. Czy naprawdę chcemy, aby operatorzy – pod pozorem inwentaryzacji oraz dbania o jakość infrastruktury – utonęli w gąszczu tabelek, raportów i urzędowych pism?



Źródło: dr MiŚOT

W informacji od UKE znajdziemy szereg problemów, na które może natknąć się zgłaszający raportować dane do Punktu Informacyjnego ds. Telekomunikacji. Czyli już wiemy, że łatwo nie będzie, a komplikacje będą się mnożyć. Złap je wszystkie, prawda?

Na ISP Forum skwitowano to dość ironicznie:

Uprzejmie przypominamy Urzędowi Komunikacji Elektronicznej, że ww. Urząd także powinien znać termin w którym to powinien udostępnić operatorom działające narzędzie, umożliwiające wywiązanie się z nałożonego na nich obowiązku....

Niektórzy operatorzy mają problemy już na dość wczesnym etapie, czyli podczas wgrywania danych do systemu. Kontakt z helpdeskiem urzędu nie pomaga. Taka sytuacja najpewniej skończy się koniecznością wysłania PIT jeszcze raz.

Natomiast temat SIDUSIS, który to w 2023 roku przysporzył wielu przedsiębiorcom z branży mnóstwo dodatkowej pracy, ucichł. Nie słyszałem, żeby nowa funkcjonalność na stronie gov.pl, czyli wyszukiwarce inwestycji szerokopasmowych planowanych na danym obszarze, cieszyła się popularnością wśród użytkowników.

Na koniec najbardziej martwiąca uwaga. Czy środowisko telekomów coś z tym jednak zrobi?

> i oczywiście nasze środowisko tylko na ten temat sobie popłacze i nic z tym nie zrobimy 😉

Jeśli ktoś uważnie nasłuchuje, co dzieje się w kuluarach związanych z tym tematem, to dowie się, że sprawy idą w dobrym kierunku. Mam nadzieję, że to kierunek dobry dla operatorów.

Z ŻYCIA MIŚOT

AUTOR
Marek Nowak

Na co idą pieniądze z Fundacji Lokalni

i dlaczego warto ją wesprzeć

Fundacja Lokalni działa na rzecz małych i średnich operatorów telekomunikacyjnych od 2019 roku. Wspiera potrzebujących, których dotknęły przykre zdarzenia losowe i choroby, promuje społeczną odpowiedzialność biznesu, działa na rzecz ograniczania negatywnego wpływu działalności przedsiębiorstw na środowisko. Od tego roku można ją wesprzeć, przekazując 1,5 proc. podatku dochodowego.

Fundatorem organizacji jest Stowarzyszenie e-Południe i dotychczasowe jej działania były finansowane głównie z jego środków. W zeszłym roku fundacja zyskała status organizacji pożytku publicznego. Oznacza to, że wszyscy, a w szczególności operatorzy i ich pracownicy, mogą przeznaczyć część swoich podatków na inicjatywy lokalne i projekty przez nią prowadzone. Podajemy numer Krajowego Rejestru Sądowego, który należy wpisać w odpowiednim polu formularza rozliczającego podatek dochodowy: KRS 0000814704.

Komu w zeszłym roku pomogła Fundacja Lokalni?

Działania Fundacji Lokalni są transparentne, a w zeszłym roku obejmowały między innymi pozycje takie jak: koszty operacji ratującej życie czy rehabilitacja po ciężkiej chorobie.

DZIAŁANIA FUNDACJI LOKALNI SĄ TRANSPARENTNE, A W ZESZŁYM ROKU OBEJMOWAŁY MIĘDZY INNYMI POZYCJE TAKIE JAK: KOSZTY OPERACJI RATUJĄCEJ ŻYCIE CZY REHABILITACJA PO CIĘŻKIEJ CHOROBIE

Fundacja wielokrotnie wspierała też działania związane ze sportową aktywnością dzieci i młodzieży: naprawę zdewastowanego piłkochwytu na boisku szkolnym (o pomoc w tym zakresie wnioskowała spółka MediaNet24), zakup koszulek dla zawodników startujących w zawodach, dofinansowanie VIII Biegu Mikołajów (Microchip) czy zakup zamku Giganta, który spłonął w trakcie pożaru garażu. Dofinansowano także projekt Wyskakuj z Laptopa (Systemia) oraz zakup sprzętu AGD dla domu dziecka w gminie Wieruszów (Comnet Multimedia).

Warto w tym miejscu przypomnieć także, że jedną z wieloletnich inicjatyw Fundacji Lokalni jest konkurs TeleOdpowiedzialny Roku.

– Jesteśmy też otwarci na rekomendacje środowiska małych i średnich operatorów telekomunikacyjnych – podkreśla Aleksandra Czerech, prezeska Fundacji Lokalni.

W zeszłym roku fundacja zyskała status organizacji pożytku publicznego.

Okazją do rozmowy o inicjatywach wartych wsparcia będzie też z pewnością zbliżający się Zjazd MiŚOT w Janowie Podlaskim, gdzie poznamy także TeleOdpowiedzialnego 2023 roku.

Z ŻYCIA MIŚOT

AUTOR
Aleksandra Czerech

Nie czekaj, dołącz do Lokalnych!

Wsparcie i łączenie sił przyświecają małym i średnim operatorom telekomunikacyjnym od dawna. Wspólne działania pozwoliły na rozwój oraz znalezienie optymalnych rozwiązań wielu problemów, z jakimi borykali się operatorzy na przestrzeni lat. Projekt Lokalni to kolejna cegiełka dająca szansę na pozyskanie nowych klientów. Jak z niej skorzystać?

Lokalni.pl to przede wszystkim wyszukiwarka, w której poszukujący usług telekomunikacyjnych łączeni są z dostawcą. W odróżnieniu od podobnych produktów dostępnych na rynku ten jest wyjątkowy – bo dedykowany małym i średnim operatorom telekomunikacyjnym.

Wyszukiwarka wspierana jest działaniami w mediach społecznościowych, gdzie prowadzone są profile Lokalnych, które znajdziecie na Facebooku oraz Instagramie. Wielu spośród MiŚOT-ów korzysta z usługi Publikon, w ramach której przygotowujemy i publikujemy posty w imieniu operatorów na ich profilach facebookowych, w najlepszej na rynku cenie. Z oferty tej można skorzystać, wybierając *wizytówkę premium* z jednym postem tygodniowo lub *premium+* – obejmującą dwie publikacje na Facebooku.

Czy wyszukiwarka to wszystko?

Lokalni.pl to dużo więcej. Poza wyszukiwarką w zakładce *o nas* znajdziecie manifest, pod którym podpisze się każdy MiŚOT. Zachęcamy do zapoznania się z jego treścią. Pod tym przesłaniem znajdują się wizytówki małych i średnich operatorów telekomunikacyjnych, które każdy z Was może edytować, wybierając wcześniej w Sklepie MiŚOT jedną z trzech dostępnych opcji. Ceny za nie są dosłownie symboliczne.

W dedykowanej zakładce znajdziecie opis usług, jakie dostarczają mali i średni operatorzy telekomunikacyjni

WIELU SPOŚRÓD MIŚOT-ÓW KORZYSTA Z USŁUGI PUBLIKON, W RAMACH KTÓREJ PRZYGOTOWUJEMY I PUBLIKUJEMY POSTY W IMIENIU OPERATORÓW NA ICH PROFILACH FACEBOOKOWYCH, W NAJLEPSZEJ NA RYNKU CENIE

swoim klientom, a w kolejnej, pod hasłem *Mapa dobra,* zalogowani użytkownicy mogą dodawać działania z zakresu CSR, czyli aktywności na rzecz lokalnej społeczności – nad tą sekcją trwają jeszcze prace.

Plany

Na najbliższy czas przewidziane są prace mające na celu podniesienie jakości sekcji usług w wizytówkach. Dodana również zostanie zakładka blog. Najważniejszą zmianą będzie pojawienie się dedykowanych podstron, czyli *dużych wizytówek*, które będą stroną operatora w serwisie lokalni.pl. Natomiast na stronach internetowych poświęconych projektom KameleonTV czy KoalaTel znajdą się odnośniki uczestników tych projektów do ich podstron w portalu Lokalni, co wpłynie pozytywnie na pozycjonowanie wszystkich tych stron.

Przygotowujemy również trzymiesięczną kampanię reklamową, która będzie wsparciem dla MiŚOT-ów. Obejmie ona lokalizacje tych małych i średnich operatorów, którzy jako pierwsi dołączyli do projektu, a jest to blisko 50 firm.

Wyszukiwarka będzie tym skuteczniejsza, im więcej MiŚOT-ów dołączy do projektu. Koszt udziału jest symboliczny między innymi po to, by ułatwić podjęcie decyzji. My w Grupie MiŚOT wierzymy w korzyści, jakie przyniesie ten projekt wszystkim małym i średnim operatorom telekomunikacyjnym. Uda się to jednak tylko wtedy, kiedy Wy, MiŚOT-y, weźmiecie w nim udział. Dołącz teraz: https://sklep.misot.pl/lokalni/.

Na najbliższy czas przewidziane są prace mające na celu podniesienie jakości sekcji usług w wizytówkach.

Projekt Lokalni.pl realizowany jest dzięki wsparciu Grupy MiŚOT.

AUTOR
Michał Koch

AI na MWC Barcelona 2024:
nowa era dla telekomunikacji

W trakcie Mobile World Congress (MWC) w Barcelonie 2024 r. tematem dominującym podczas prezentacji jest bez wątpienia sztuczna inteligencja. Firmy telekomunikacyjne i dostawcy sprzętu już teraz analizują możliwości, jakie sztuczna inteligencja otwiera przed branżą telekomunikacyjną, zastanawiając się nad korzyściami i ryzykiem związanym z jej wdrożeniem.

Rahul Kumar, główny konsultant IBM ds. globalnych rozwiązań telekomunikacyjnych, podkreślił, że AI jest najczęściej omawianym tematem na targach. Wskazał, że obecna technologia AI umożliwia firmom szybsze wejście na rynek dzięki większej łatwości w uzyskiwaniu wyników i przystępnemu użytkowaniu. Konsumeryzacja narzędzi takich jak ChatGPT sprawia, że coraz więcej osób jest zaznajomionych z korzystaniem z AI. Przekłada się to na rozważania o potencjalnym znaczeniu sztucznej inteligencji dla firm.

IBM, według Kumara, już współpracuje z klientami z branży, wykorzystując sztuczną inteligencję do obsługi klienta czy tworzenia kodu. Firma rozwija także zastosowania AI w operacjach sieciowych, gdzie inżynierowie mogą korzystać z interfejsu języka naturalnego do rozwiązywania problemów sieciowych, opierając się na wiedzy zgromadzonej z różnych podręczników technicznych.

Michael Dell, prezes i dyrektor generalny Dell Technologies, zauważył, że potencjał AI jest ogromny i rozwija się w niespotykanym dotąd tempie. Porównując AI do prasy drukarskiej, zwrócił uwagę na jej zdolność do kreowania zupełnie nowej gospodarki opartej na informacji. Jednak szybkość rozwoju AI rodzi pytania dotyczące etyki i zarządzania, zwłaszcza w kontekście konieczności regulacji i monitorowania modeli AI.

Na MWC firma Aira Technologies zaprezentowała demo RAN GPT, modelu służącego do wykonywania zapytań i kontrolowania sieci dostępu radiowego, pokazując możliwości operacyjne AI oraz wdrożone mechanizmy bezpieczeństwa.

FIRMA ROZWIJA TAKŻE ZASTOSOWANIA AI W OPERACJACH SIECIOWYCH, GDZIE INŻYNIEROWIE MOGĄ KORZYSTAĆ Z INTERFEJSU JĘZYKA NATURALNEGO DO ROZWIĄZYWANIA PROBLEMÓW SIECIOWYCH, OPIERAJĄC SIĘ NA WIEDZY ZGROMADZONEJ Z RÓŻNYCH PODRĘCZNIKÓW TECHNICZNYCH

Microsoft, reprezentowany przez wiceprezesa i prezesa Brada Smitha, przedstawił zasady dotyczące zarządzania infrastrukturą centrum danych AI i innych zasobów AI, podkreślając znaczenie dostępu do AI w promowaniu innowacji i wspieraniu wolnej konkurencji. Ogłoszono również inwestycje w wysokości około 5,6 mld USD w centra danych AI i chmurę w Europie, co stanowi największą inwestycję firmy w Hiszpanii.

Tegoroczne MWC pokazało, że sztuczna inteligencja staje się kluczowym elementem ekosystemu telekomunikacyjnego, mającym potencjał do przekształcenia sposobu, w jaki przetwarzane, zarządzane i wykorzystywane są dane. Chociaż transformacja sektora z wykorzystaniem AI jest jeszcze przed nami, jasne jest, że sztuczna inteligencja będzie miała znaczący wpływ na branżę telekomunikacyjną.

TELEWIZJA

AUTOR
Wojciech Szymczak

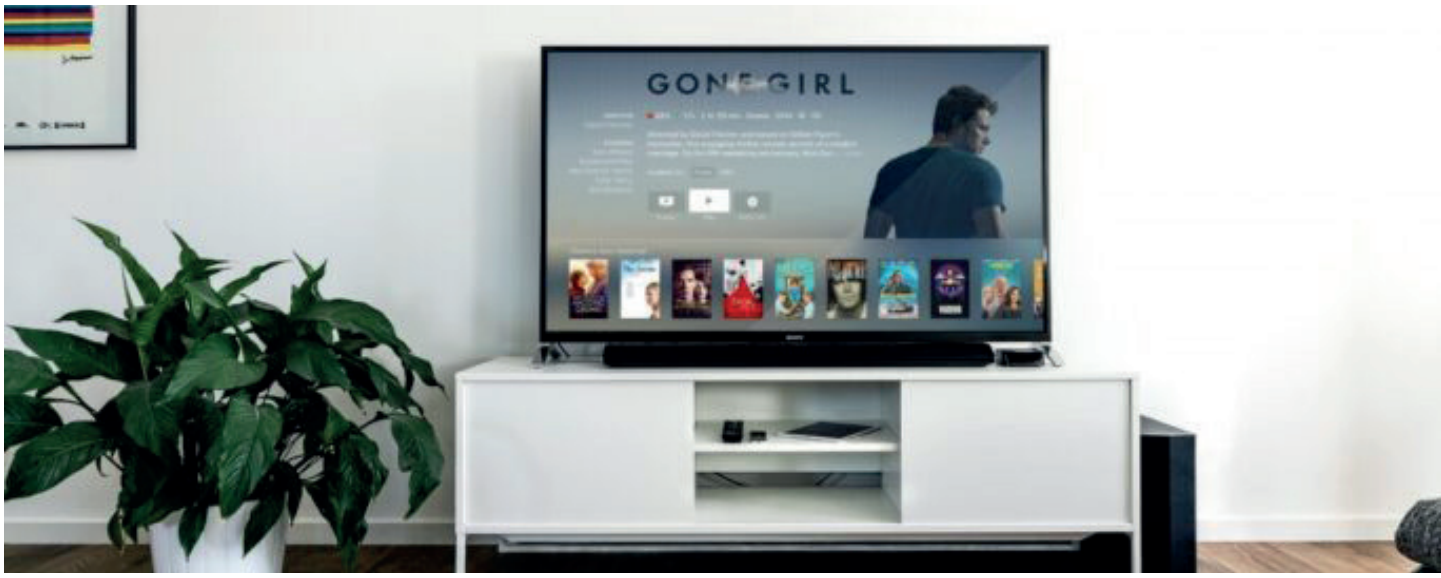
Wynagrodzenia za VOD
– czy w końcu pojawią się tantiemy?

15 lutego 2024 roku opublikowany został projekt ustawy nowelizującej prawo autorskie w celu wdrożenia dyrektyw 2019/789 i 2019/790. Polska jest w tym zakresie spóźniona już 3 lata. Pierwotna wersja projektu powstała jeszcze w 2022 roku, ale w 2023 roku utknęła w poprzednim rządzie. Dlaczego?

Między Ministerstwem Cyfryzacji i Ministerstwem Finansów pojawił się spór związany z wprowadzeniem dodatkowego wynagrodzenia (tantiem autorskich) za korzystanie z dzieł audiowizualnych na polu eksploatacji VOD (Video On Demand). Aktualny projekt nie zawiera już tego kontrowersyjnego przepisu. Temperatura sporu jednak nie opadła, lecz poszybowała do niespotykanych dotąd poziomów.

Stowarzyszenie Filmowców Polskich złożyło do Prokuratury Okręgowej w Warszawie zawiadomienie o podejrzeniu popełnienia przestępstwa polegającego na zaniechaniu przyjęcia dyrektywy unijnej wprowadzającej tantiemy z internetu. Podejrzanymi mają być członkowie poprzedniego rządu, ale w świetle kształtu aktualnego rządowego projektu ustawy (bez dodatkowych wynagrodzeń za VOD) można założyć, że także obecny rząd może znaleźć się na celowniku śledczych, a przynajmniej zostanie wskazany prokuraturze przez SFP, chyba że przestępstwem było jedynie spotkanie się przez premiera Mateusza Morawieckiego z ówczesnym szefem Netflixa, które – zdaniem środowiska filmowców – dało impuls do zablokowania w rządzie tantiem za VOD.

Warto dodać, że to SFP, jako organizacja zbiorowego zarządzania, pobierałaby te wynagrodzenia na rzecz współtwórców utworów audiowizualnych. Działa aktywnie na wielu polach, snując wizję obowiązku ich ustanowienia, wynikającą rzekomo z art. 18 dyrektywy 2019/790. Tym samym zdaje się stawiać znak równości: wdrożona dyrektywa = tantiemy za VOD. Na stronie tantiemyzinternetu.pl (domena zarejestrowana na SFP) prezentuje mapę, z której wynika, że na całym kontynencie tylko Polska nie wdrożyła unijnej dyrektywy do prawa krajowego. Czy to znaczy, że w każdym państwie



TEMPERATURA SPORU JEDNAK NIE OPADŁA, LECZ POSZYBOWAŁA DO NIESPOTYKANYCH DOTĄD POZIOMÓW

członkowskim UE współtwórcy utworu audiowizualnego i artyści wykonawcy są uprawnieni do dodatkowego i niezbywalnego wynagrodzenia od VOD? Takie spekulacje rząd ucina w uzasadnieniu projektu:

W ramach implementacji omawianego art. 18 dyrektywy w niektórych, aczkolwiek nielicznych państwach wprowadzono na rzecz twórców lub wykonawców niezbywalne i wykonywane za pośrednictwem organizacji zbiorowego zarządzania prawo do wynagrodzenia z tytułu publicznego udostępniania utworu audiowizualnego w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym.

W istocie art. 18 ust. 2 dyrektywy 2019/790 wprost wskazuje, że państwa członkowskie mają dowolność w wyborze mechanizmu, który zastosują, aby twórcy i wykonawcy mieli prawo do odpowiedniego i proporcjonalnego wynagrodzenia. Ponadto wdrażając dyrektywę, trzeba uwzględniać zasadę swobody zawierania umów oraz sprawiedliwą równowagę praw i interesów. Polska liczy zatem na wprowadzane przez samych dostawców VOD systemy dodatkowego wynagradzania twórców i wykonawców w przypadkach, gdy dany film czy serial uzyska określony próg sukcesu komercyjnego. Jednocześnie zastrzega się, że jeżeli podobne systemy wynagradzania nie będą funkcjonować w sposób zadowalający, konieczna może okazać się w przyszłości interwencja ustawodawcy.

Więcej aktualnych informacji ze świata telekomunikacji dostępnych jest także w Biuletynie kancelarii Prawnej Media. Zapisz się, by być na bieżąco! https://kancelaria.media.pl/biuletyn/

JAMBOX

TELEWIZJA ŚWIATŁOWODOWA

www.jambox.pl

tv smart

DEKODERY IPTV

Arris 4302 HD

Arris 5202 4K

CatchUp
7 DNI WSTECZ

StartOver
OGLĄDAJ OD POCZĄTKU

JAMBO Nagrywarka
NAGRYWAJ W CHMURZE

tv smart GO

NOWOŚĆ!

ZAMÓW TERAZ NA BEZPŁATNE TESTY
sgt.net.pl

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

TV Smart to także:

- Telewizja linearna z funkcjami StartOver i CatchUp
- Nagrywanie w chmurze lub na dysku USB
- Pilot bluetooth z możliwością głosowej obsługi
- Wbudowane Wi-Fi i Chromecast
- Aplikacja TV Smart GO na urządzenia mobilne (Android, iOS), telewizory LG, Samsung oraz w przeglądarkach internetowych.

TELEFONIA KOMÓRKOWA

JAMBOX mobile

LTE 5G

VoLTE Wi-Fi Calling

Blisko **300** kanałów, w tym **185** 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

- 16 lat na rynku IPTV, 570 partnerów ISP
- 160 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 mobilny Internet LTE i 5G, proste przenoszenie numerów, rozmowy z prędkością technologii LTE i zawsze pewny zasięg dzięki Wi-Fi Calling

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

TELEWIZJA

AUTOR
Klaudia Wojciechowska

Prokuratorzy szkolą się z piractwa IPTV i sharingu

300 prokuratorów z całej Polski zapoznało się z kwestiami piractwa IPTV i sharingu w ramach szkolenia przygotowanego przez antypirackie Stowarzyszenie Sygnał. Przedstawiono techniczne aspekty zwalczania przestępstw związanych z nielegalnym streamingiem i sharingiem. Organizacja przeprowadziła badania, z których wynika, że w naszym kraju rocznie dochodzi do 6,1 mln przypadków nielegalnej dystrybucji treści.

Stowarzyszenie Sygnał jest partnerem w tworzeniu szkoleń wraz z Departamentem do Spraw Cyberprzestępczości i Informatyzacji Prokuratury Krajowej. Szkolenia dla prokuratorów obejmują zagadnienia takie jak:

- techniczne aspekty organizowania przestępczości związanej ze streamingiem;
- techniczne aspekty organizowania przestępczości związanej z sharingiem, czyli dzieleniem się uprawnieniami na dekoderach satelitarnych;
- IPTV;
- przegląd narzędzi stosowanych w ramach OSINT;
- metody wyliczenia szkody;
- najnowsze orzecznictwo i przegląd najciekawszych spraw.

Szkolenia są jednym z elementów przygotowujących do planowanego wdrożeniem wytycznych w zakresie prowadzenia spraw, w obszarze streamingu.

– Od lat staramy się wspierać organy ścigania swoją wiedzą ekspercką w zakresie naruszeń praw do treści audiowizualnych online, co przekłada się na skuteczność i sprawność prowadzonych postępowań. W zeszłym roku zrealizowaliśmy ogólnopolski cykl szkolenia dla funkcjonariuszy policji specjalizujących się w zagadnieniach związanych z kradzieżą treści audiowizualnych w internecie. Jednym z naszych priorytetów na 2024 rok jest wzmocnienie współpracy z Prokuraturą Krajową, ale także z Krajową Szkołą Sądownictwa i Prokuratury – zapewniła Teresa Wierzbowska, prezeska Stowarzyszenia Sygnał.

Skala piractwa w Polsce

W roku 2024 może nastąpić przełom w standaryzacji mechanizmów ochrony własności intelektualnej w Europie. Wzrasta świadomość wartości praw autorskich. To przekłada się na wdrażanie coraz bardziej zaawansowanych mechanizmów reagowania na nielegalną dystrybucję treści w internecie.

Komisja Europejska wydała w tej sprawie rekomendacje i w 2024 r. będzie badane ich stosowanie. Ma to prowadzić do wprowadzenia skutecznych rozwiązań. Stowarzyszenie Sygnał postanowiło uchwycić kluczowe kwestie, które bada KE. Wnioski umieściło w raporcie.

W okresie od września 2022 roku do sierpnia 2023 roku odnotowano 6,1 miliona przypadków nielegalnej dystrybucji treści audiowizualnych. Dotyczyło to głównie VOD. Przekłada się to na nielegalną dystrybucję każdego materiału ponad 3600 razy rocznie, czyli 10 razy dziennie.

Według oceny Stowarzyszenia Sygnał mechanizmy zgłaszania naruszeń nie są w pełni efektywne. Około 34 proc. zgłoszeń to tzw. *zgłoszenia iluzoryczne*. Treści, pomimo ich usunięcia ze zgłaszanego miejsca, pojawiają się w nich ponownie.

Jeśli zaś idzie o naruszenia praw dystrybucji wydarzeń na żywo, to aż 94 proc. zgłoszeń nie przynosiło żadnego rezultatu. Tylko 5 proc. tego typu zgłoszeń skierowanych do serwisów pirackich było rozpatrywanych w ciągu 30 minut od ich przekazania. Jest to poważne wyzwanie dla skutecznego zwalczania nielegalnej dystrybucji treści audiowizualnych w czasie rzeczywistym.

Stowarzyszenie Sygnał ocenia, że w związku z tym w Polsce jest jeszcze wiele do zrobienia w celu ochrony przed działaniami piracki mi. Przede wszystkim sporo pracy trzeba wykonać, by dostosować realia do wdrażanych w Europie mechanizmów live blocking.

WZRASTA ŚWIADOMOŚĆ WARTOŚCI PRAW AUTORSKICH. TO PRZEKŁADA SIĘ NA WDRAŻANIE CORAZ BARDZIEJ ZAAWANSOWANYCH MECHANIZMÓW REAGOWANIA NA NIELEGALNĄ DYSTRYBUCJĘ TREŚCI W INTERNECIE

STOWARZYSZENIE SYGNAŁ OCENIA, ŻE W ZWIĄZKU Z TYM W POLSCE JEST JESZCZE WIELE DO ZROBIENIA W CELU OCHRONY PRZED DZIAŁANIAMI PIRACKIMI

To blokowanie dostępu do nielegalnych transmisji w trybie natychmiastowym, czyli w czasie do 30 minut. Takie rozwiązania wprowadzono już we Włoszech czy Hiszpanii, ale Polska wciąż ma z tym problem. Sprawa dotyczy, chociażby nielegalnych transmisji wydarzeń sportowych.

Obecna sytuacja rozpowszechnienia streamingu sprawia, że piractwo jest łatwiejsze niż kiedykolwiek. Wciąż powstają nowe strony internetowe, które przypominają legalnie działających operatorów, ale takimi nie są. Oferują dostęp do kanałów telewizyjnych, transmisji sportowych i produkcji wideo na żądanie, przekierowując treści z różnych platform.

Całkowite wyeliminowanie piractwa wydaje się niemożliwe.

Całkowite wyeliminowanie piractwa wydaje się niemożliwe. Także dlatego, że w sklepie Google Play na Android TV znaleźć można wiele aplikacji, które służą do odtwarzania nielegalnych list m3u. Jednak fakt, że walka z tym jest trudna, nie oznacza, że nie należy jej podjąć.

ZARZĄDZANIE

AUTOR
Klaudia Wojciechowska

Dostępność BOK-ów
dla osób z niepełnosprawnościami

Urząd Komunikacji Elektronicznej sprawdził biura obsługi klientów największych ogólnopolskich operatorów telekomunikacyjnych oraz kilku lokalnych. Badanie miało na celu ocenę zapewnienia udogodnień dla osób z niepełnosprawnościami.

Jak dostosować BOK do potrzeb osób z niepełnosprawnościami?

Firmy telekomunikacyjne mają obowiązek zapewnić następujące udogodnienia osobom z niepełnosprawnościami:

- możliwość wjazdu do punktu obsługi klienta czy salonu na wózku;
- faktury, informacje, dokumenty w alfabecie Braille'a;
- rozmowa z doradcą klienta za pośrednictwem tłumacza polskiego języka migowego;
- możliwość otrzymania mailem dokumentów, które odczyta program czytający;
- pomoc przy skonfigurowaniu ustawień telefonu czy tabletu;
- możliwość zakupu urządzenia końcowego, przystosowanego do używania przez osoby z niepełnosprawnością słuchu.

Pracownicy Urzędu Komunikacji Elektronicznej w każdym roku sprawdzają, czy firmom telekomunikacyjnym udaje się te rozwiązania wdrożyć. W latach 2018-2023 przeprowadzono kontrole w 241 Biurach Obsługi Klienta (BOK) w całej Polsce.

W ubiegłym roku kontrola odbyła się od 4 do 29 września 2023 r. Sprawdzono BOK-i czterech największych ogólnopolskich operatorów mobilnych (łącznie 44 BOK-i) oraz ośmiu operatorów lokalnych. W ich przypadku było to po jednym obiekcie.

W trakcie kontroli analizowano elementy, takie jak:

- oznakowanie BOK;
- dostępność architektoniczna;

- świadczone udogodnienia;
- obsługa osób niesłyszących i niemówiących;
- obsługa osób niewidomych i słabowidzących;
- dostęp do urządzeń końcowych.

Wnioski z kontroli – operatorzy lokalni bez uchybień

Po kontroli przeprowadzonej w 2023 r. stwierdzono, że głównym obszarem wymagającym podnoszenia standardów w zakresie obsługi osób z niepełnosprawnością jest obszar architektoniczny. W 21 BOK-ach stwierdzono istnienie stanowisk, które utrudniają dostęp i obsługę dla osób z niepełnosprawnościami z powodu niedostosowania wysokości biurka lub zbyt małą przestrzeń pod blatem biurka. W dwóch przypadkach utrudnione było dotarcie do takiego stanowiska.

W sześciu BOK-ach operatorów mobilnych stwierdzono nieprawidłowości skutkujące wydaniem zaleceń pokontrolnych, które nakazują operatorom P4 sp. z o.o. i T-Mobile Polska S.A. usunięcie stwierdzonych nieprawidłowości.

Po kontroli dla 26 BOK-ów operatorów ogólnopolskich Prezes UKE wydał nie tylko zalecenia pokontrolne, ale także wystosował rekomendacje wskazujące na obszary obsługowe wymagające podnoszenia standardów w zakresie obsługi osób z niepełnosprawnością. Otrzymali je wszyscy czterej najwięksi operatorzy: Orange Polska S.A., Polkomtel sp. z o.o., P4 sp. z o.o. oraz T-Mobile Polska S.A.

W przypadku BOK-ów operatorów lokalnych nie stwierdzono uchybień skutkujących wydaniem zaleceń pokontrolnych lub rekomendacji w zakresie poprawy obsługi osób z niepełnosprawnościami.

Każdy z dużych operatorów, u których po kontroli stwierdzono uchybienia, musi teraz podjąć działania w zakresie zmian wyposażenia i aranżacji architektonicznej BOK, w którym świadczona jest obsługa osób z niepełnosprawnościami. Wymagane jest również podniesienie wiedzy pracowników BOK-ów i jakości obsługi osób ze szczególnymi potrzebami.

UKE NIE TYLKO SPRAWDZA PRZESTRZEGANIE PRZEPISÓW, ALE WYZNACZA WEWNĘTRZNE I ZEWNĘTRZNE STANDARDY

Standardy obsługi osób z niepełnosprawnościami

UKE nie tylko sprawdza przestrzeganie przepisów, ale wyznacza wewnętrzne i zewnętrzne standardy.

W 2020 roku we współpracy z Fundacją Integracja Rekomendacje zostały opracowane wytyczne dla operatorów telekomunikacyjnych i pocztowych, zebrane w dokumencie *Łączność – telekomunikacja i poczta dla osób ze szczególnymi potrzebami.*

Dokument wskazuje kierunki zmian i rozwiązania, które pozwolą na zapewnienie dostępności usług dla różnych grup użytkowników niezależnie od ich wieku, płci, parametrów fizycznych, stopnia sprawności, przyzwyczajeń, preferencji oraz innych czynników.

AUTOR
Michał Koch

Cyberfront w Europie

W 2023 roku, w kontekście rosnących cyberzagrożeń, Polska stała się jednym z głównych celów ataków typu advanced persistent threats (APT) w Europie. Wśród różnorodnych niebezpieczeństw trzeba wyróżnić ataki typu ransomware – Europa jest drugim najczęściej atakowanym obszarem na świecie. Wyniki badań analityków z holenderskiego Group-IB wskazują, że cyberprzestrzeń staje się coraz bardziej niebezpiecznym miejscem.

Polska musi stawić czoła nie tylko tradycyjnym zagrożeniom, ale również tym bardziej wyrafinowanym, często sponsorowanym przez wrogie mocarstwa. To uwydatnia konieczność rozwijania zaawansowanych zdolności cyberobronnych, aby zabezpieczyć kluczowe sektory kraju przed kolejnymi zagrożeniami.

Wspomniany raport Gropu-IB ujawnił skalę zagrożeń cybernetycznych w Europie. Liczba ataków ransomware wzrosła o ponad 50 proc., dotykając firmy z różnych sektorów, w tym produkcji, nieruchomości i transportu. Polska, jako jeden z krajów najczęściej atakowanych przez cyberprzestępców, doświadczyła aż 11 pełnoskalowych ataków kontrolowanych przez grupy hakerskie wspierane przez obce – i najczęściej reżimowe – państwa.

Co więcej, instytucje rządowe i wojskowe w Polsce stały się szczególnie podatne na ataki, na co wskazuje zwiększona aktywność grup APT. Te ataki nie tylko zagrażają prywatności i bezpieczeństwu danych, ale także bezpośrednio wpływają na stabilność kraju i sytuację geopolityczną.

Epidemia zagrożeń

Ransomware nadal stanowi kluczowe zagrożenie dla europejskiego rynku. Europa, jako drugi najczęściej atakowany regionem na świecie pod względem ransomware, staje w obliczu niecodziennego wyzwania. w gestii politycznych decydentów jest to, czy zdołamy się obronić. Przygotowanie strategii walki w cyberprzestrzeni może być naszym być albo nie być. W Polsce liczba ataków ransomware wzrosła o 73 proc., czyniąc kraj jednym z najczęściej atakowanych.

EUROPA, JAKO DRUGI NAJCZĘŚCIEJ ATAKOWANY REGIONEM NA ŚWIECIE POD WZGLĘDEM RANSOMWARE, STAJE W OBLICZU NIECODZIENNEGO WYZWANIA

Jednakże nie tylko złośliwe oprogramowanie jest problemem. Grupy hakerskie stosujące wyrafinowane techniki kradzieży informacji stanowią poważne zagrożenie dla naszego krajobrazu cybernetycznego. W Europie ponad 250 000 urządzeń zostało zainfekowanych, a ich logi zostały udostępnione na darkwebowych serwerach, zagrażając prywatności i bezpieczeństwu danych użytkowników.

Rosnąca liczba ofert sprzedaży kluczy dostępu do zainfekowanych urządzeń wskazuje na coraz większe wyrafinowanie działań przestępczych. Polska, podobnie jak inne kraje Starego Kontynentu, staje się areną walki w cyberprzestrzeni. Popularność RaaS (Ransomware as a Service) powinna być alarmem dla wszystkich specjalistów od bezpieczeństwa sieci. Również zwiększanie świadomości społeczeństwa powinno być jednym z fundamentów obrony.

Niepokojące jest pojawienie się nowych graczy na scenie cyberprzestępczej, takich jak mazikeen, którzy oferują dostęp do korporacyjnych sieci za pośrednictwem różnych metod, w tym zainfekowanych kont zdalnego pulpitu RDP. To tylko kolejny z przykładów tego, jak dynamiczny i zróżnicowany staje się świat cyberprzestępczości.

Utrzymać cyberfront

W obliczu tych wyzwań, kluczowe jest podjęcie natychmiastowych działań przez rząd i sektor prywatny. Inwestycje w nowoczesne technologie bezpieczeństwa, wzmocnienie przepisów regulujących ochronę danych oraz edukacja społeczeństwa na temat zagrożeń cybernetycznych są kluczowe, aby skutecznie przeciwdziałać atakom i chronić bezpieczeństwo Polski.

W świetle tych danych staje się jasne, że nasz kraj stoi w obliczu poważnych wyzwań związanych z cyberbezpieczeństwem. Konieczne są dalsze działania na poziomie krajowym i międzynarodowym, aby zapewnić ochronę przed atakami hakerskimi i zapewnić bezpieczeństwo danych obywateli oraz instytucji. Walka w cyberprzestrzeni staje się nie mniej istotna niż walka na tradycyjnych frontach.

Operatorów zainteresowanych zagadnieniami dot. cyberbezpieczeństwa zachęcam do zapoznania się z działaniami projektu MdS.

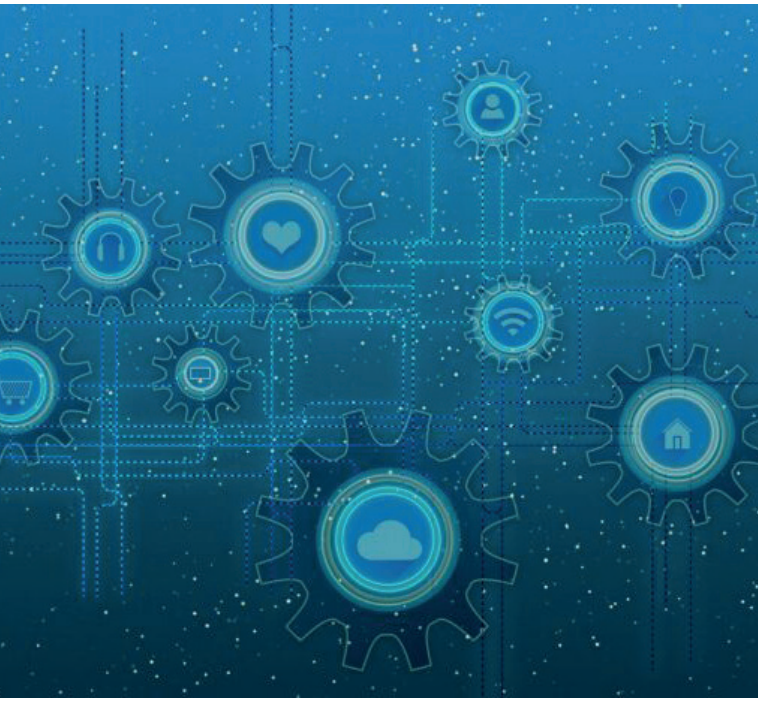
TECHNOLOGIE

AUTOR
Marek Nowak

Ministerstwo wznowiło pracę GRAI i GRIoT

Grupy robocze związane z internetem rzeczy i sztuczną inteligencją działały już w poprzedniej kadencji rządu. Ministerstwo Cyfryzacji kontynuuje ich spotkania, choć ze względu na pokrewieństwo tematów nie wiadomo jeszcze, ile grup ostatecznie podejmie pracę.

– Skorzystaliśmy z zaproszenia na spotkanie Grupy Roboczej ds. AI, IoT i technologii organizowane przez ministerstwo. Wziąłem w nim udział, ponieważ zależy nam na tym, by rozwój tych technologii w Polsce brał pod uwagę także rozwiązania z zakresu LoRaWAN, bliskie małym i średnim operatorom telekomunikacyjnym i już przez nich wdrażane – mówi Łukasz Biernacki z Grupy MiŚOT. – Spotkanie wznawiało prace grupy, służyło prezentacji stanowisk i zmierzało do wypracowania nowej formuły działania.



Ministerstwo Cyfryzacji od pewnego czasu deklaruje szczególne zainteresowanie działaniami, których celem jest rozwijanie sztucznej inteligencji i opartej na niej innowacji. Zainteresowanych tym obszarem nie brakuje, o czym można było przekonać się 26 lutego w siedzibie MC. Wiele osób uczestniczyło w nim również online.

Niebawem możemy spodziewać się określenia, jakie kierunkowe zmiany powinny nastąpić w dokumencie Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020 (choć zastanawiające jest, dlaczego ministerstwo wciąż operuje materiałami z tak nieaktualną datą) oraz podsumowania sugestii uczestników spotkania w wątku usprawniania działania ekosystemu AI w Polsce. Uczestnicy proszeni byli także o sugestie dotyczące tego, jakie jeszcze inicjatywy powinno podejmować Ministerstwo Cyfryzacji w obszarze technologii przełomowych – AI, IoT, Quantum, Blockchain, HPC.

Trudno w tym momencie nie zadać podstawowego pytania dotyczącego tego zagadnienia, które brzmi: Czy w ogóle powinno? Jak już komentowaliśmy na

MINISTERSTWO CYFRYZACJI OD PEWNEGO CZASU DEKLARUJE SZCZEGÓLNE ZAINTERESOWANIE DZIAŁANIAMI, KTÓRYCH CELEM JEST ROZWIJANIE SZTUCZNEJ INTELIGENCJI I OPARTEJ NA NIEJ INNOWACJI

łamach ISPortalu sny o europejskiej potędze technologicznej miało przed nami wiele krajów i jeszcze więcej firm. Europa w dalszym ciągu nie doczekała się własnego odpowiednika Doliny Krzemowej, a problem w tym zakresie może być poważniejszy, systemowy i wynikać właśnie ze zbyt dużego interwencjonizmu państwowego.

Europa w dalszym ciągu nie doczekała się własnego odpowiednika Doliny Krzemowej

Warto też zaznaczyć, że grupa uczestników spotkania reprezentowała szerokie spektrum – przedsiębiorców, dostawców technologii, przedstawicieli nauki, etyków, prawników oraz organizacje pozarządowe.

FELIETON

AUTOR
Michał Koch

Dla ucznia laptop, dla ministerstwa kłopot

Laptopów dla uczniów nie będzie, bo nie ma na to kasy. Jednocześnie w magazynach zalega 10 tys. komputerów przenośnych, które nie trafiły do rąk najmłodszych. Czy program walki z cyfrowym wykluczeniem zamienił się właśnie w jeden wielki chaos?

Na program Laptop dla ucznia – warto zaznaczyć, że powstały za rządów PiS – przeznaczono 1,15 mld PLN. Sprzęt miał trafić do rąk uczniów klas czwartych. Niby obyło się bez większych kontrowersji, a sama specyfikacja techniczna laptopów nie należała do najgorszych. Po zmianie władzy audyt wykazał, że w magazynie Naukowej i Akademickiej Sieci Komputerowej (NASK) zalega 10 tys. pudełek z nowym sprzętem.

W styczniu minister cyfryzacji Krzysztof Gawkowski poinformował, że program nie będzie kontynuowany. Powodem są nieprawidłowości w zabezpieczeniu finansowania. Polityk przekazał, że dotychczas za laptopy płacono środkami z KPO, ale nie na zasadach, które przyjął PiS. Chodzi m.in. o dopuszczenie do pełnej własności urządzeń po okresie pięciu lat, czy rozdawanie ich bez spełniania żadnych wymogów.

Podczas audytu wyszło na jaw, że ministrowie z PiS wiedzieli o problemie. Z ujawnionego dokumentu wynika, że Komisja Europejska nie zaakceptowała zmian zaproponowanych przez Ministerstwo Cyfryzacji oraz negatywnie oceniła sposób realizacji programu przez ministerstwo edukacji.

Dariusz Standerski, sekretarz stanu w resorcie cyfryzacji, informuje:

– Poza tym, że zidentyfikowaliśmy nieprawidłowości związane z przygotowaniem całego procesu, to bardzo boli mnie fakt, że w tym pośpiechu, w tym braku przygotowania, w ustawie o laptopach nie przewidziano, co można zrobić z tymi komputerami, które zostaną zwrócone.

EKSPERCI WSKAZUJĄ, ŻE BRAK OPROGRAMOWANIA ZABEZPIECZAJĄCEGO KOMPUTERY PRZED ZŁOŚLIWYM OPROGRAMOWANIEM TO PROSZENIE SIĘ O KŁOPOTY

Zdaniem Standerskiego ówczesna władza napisała zasady programu na kolanie. Brakuje regulacji, która pozwalałaby przekazać zwrócony (lub niepobrany) komputer innemu uczniowi. Przez to tysiące laptopów kurzy się w magazynie.

– Laptopy to jest taki sprzęt, który z dnia na dzień traci na wartości – dodaje Standerski.

Resort cyfryzacji złożył też niejawne zawiadomienie do prokuratury w związku z programem. Śledczy będą sprawdzać, czy politycy odpowiedzialni za przygotowanie zasad nie dopuścili się zaniedbań.

Minister cyfryzacji nie szczędzi słów krytyki:

– Przetarg realizowano od października 2022 roku. W połowie sierpnia wybrano wykonawców, ale w międzyczasie dochodziło do spraw, które powinniśmy omówić. Wszystko wskazuje na to, że podczas przetargu doszło do naruszenia przepisów karnych, mogło dojść do korupcji.

– To była kiełbasa wyborcza dla Prawa i Sprawiedliwości. Laptopy były niezabezpieczone przed niewłaściwym użyciem, narażały dzieci na cyberzagrożenia – dodaje ministerka edukacji Barbara Nowacka.

Zdaniem Nowackiej polskiej szkole potrzebna jest mądra cyfryzacja. Ciężkie laptopy w plecakach czwartoklasistów budzą wątpliwości polityków resortu edukacji oraz nauczycieli, a brak odpowiedniej strategii cyberbezpieczeństwa może przynieść więcej szkody niż pożytku.

Do sprawy odniósł się też Marcin Zemła, pełnomocnik ds. cyberbezpieczeństwa Grupy MiŚOT:

– Jak można rozdać sprzęt z systemem operacyjnym bez uprzedniej prekonfiguracji, wiedząc, że zostanie on podpięty różnymi metodami, ale jednak do sieci publicznej? Mamy przecież KSC i obowiązek szacowania ryzyka! Czy ministerstwo chciało w ten sposób zrobić pentest środowiska szkolnego?

Eksperci wskazują, że brak oprogramowania zabezpieczającego komputery przed złośliwym oprogramowaniem to proszenie się o kłopoty. Narażeni mogą być zarówno uczniowie, jak i ich rodzice. W ramach szkolnych lekcji należałoby również poruszyć wśród najmłodszych temat cyberbezpieczeństwa.

Program naprawczy ma wkrótce zostać zapowiedziany przez przedstawicieli obu resortów. Kontynuacja Laptopa dla ucznia wymaga znalezienia w budżecie państwa dodatkowego miliarda złotych.

– Ostateczną decyzję ma podjąć premier Tusk – słyszymy z ust polityków partii rządzących.

Zatem, jeśli nie będzie laptopów dla najmłodszych, to znowu będzie to wina Tuska?

AUTOR
Michał Koch

Kto straszy AI?

Sztuczna inteligencja rozwija się w zawrotnym tempie, budząc zarówno fascynację, jak i obawy. Niektórzy eksperci, jak Jensen Huang, szef Nvidii, wieszczą śmierć kodowania i sugerują, że ludzie powinni skupić się na bardziej praktycznych umiejętnościach, takich jak rolnictwo. Inni ostrzegają przed masowym bezrobociem, gdyż boty zastąpią ludzi w pracy.

Wypowiedź Huanga jest bez wątpienia prowokująca. Przecież kodowanie było uważane za kluczową umiejętność przyszłości jak język angielski czy matematyka. Czy rzeczywiście jest aż tak niezbędne, jak nam się wydaje?

Szef Nvidii wyraźnie wskazuje, że sztuczna inteligencja jest w stanie przejąć wiele zadań, które obecnie wymagają interwencji.

AI z pewnością zautomatyzuje wiele powtarzalnych i rutynowych czynności, co może doprowadzić do utraty miejsc pracy, w takich sektorach jak transport, logistyka, produkcja czy gastronomia. Już teraz obserwujemy wdrażanie autonomicznych pojazdów, robotów kuchennych i chatbotów, które zastępują ludzi. Stwarza to też nowe możliwości dla firm i zapotrzebowanie na specjalistów, w takich dziedzinach jak: programowanie, tworzenie algorytmów, analiza danych, cyberbezpieczeństwo czy etyka AI. Potrzeba też będzie kreatywnych i empatycznych pracowników, którzy potrafią budować relacje i rozwiązywać problemy. Tego AI nie potrafi.

Polska w strachu

Według raportu Polskiej Agencji Rozwoju Przedsiębiorczości (PARP) z 2024 roku, aż 58 proc. Polaków uważa, że AI może odebrać im pracę w przyszłości. Jednocześnie, badanie Deloitte z 2023 roku pokazuje, że 38 proc. użytkowników AI już teraz obawia się, że zostanie przez nią zastąpione. Co ciekawe, co piąty użytkownik inteligentnych algorytmów deklaruje, że korzysta z niej w celach zawodowych.

Natomiast najnowsze analizy EY i Liberty Global ujawniają, że prawie połowa miejsc pracy nad Wisłą może skorzystać z wprowadzenia sztucznej inteligencji. Dlaczego? Ponieważ tyle samo stanowisk pracy w Polsce opiera się na dobrze funkcjonujących sieciach i technologiach.

Innymi słowy, AI posiada duży potencjał do wspierania rodzimej gospodarki, ale aby ten potencjał stał się rzeczywistością, niezbędna jest solidna infrastruktura oraz odpowiednio wyszkoleni pracownicy. To jednak nie wszystko.

Jak przetrwać?

Kluczem do przetrwania rewolucji AI jest adaptacja i przekwalifikowanie. Zamiast kurczowo trzymać się tradycyjnych zawodów, musimy być gotowi na zmianę i zdobycie nowych umiejętności. Pomocą w tym mogą być kursy online, programy i szkolenia oferowane przez firmy i instytucje edukacyjne.

W najnowszym raporcie firma analityczna McKinsey przestrzega przed dalszym spadkiem zatrudnienia spowodowanym AI. Przewiduje się, że aż 75 proc. rutynowych zadań może zostać zautomatyzowanych. Call center, obsługa klienta, a nawet praca w gastronomii – wszystko to może zostać przejęte przez sztuczną inteligencję. To dopiero początek.

Badania IBM wskazują, że około 40 proc. pracowników będzie musiało podlegać przekwalifikowaniu się w ciągu najbliższych trzech lat. Jednakże menedżerowie wskazują, że sztuczna inteligencja raczej rozszerzy zakres kompetencji pracowników, niż ich zastąpi. W końcu osoby, które przystosują się do pracy w środowisku sztucznej inteligencji, mogą oczekiwać premii w wysokości 15 proc.

Zysk rośnie, ale co z pracownikami?

AI jest postrzegana jako narzędzie do budowania pozytywnych relacji z pracą. W rozwijających się gospodarkach 76 proc. pracowników umysłowych uważa, że AI uczyni ich pracę łatwiejszą, a 75 proc. twierdzi, że będzie ona bardziej interesująca. W porównaniu do 48proc. i 44 proc. w dojrzałych gospodarkach te statystyki pokazują duży potencjał AI w poprawie komfortu pracy.

W ROZWIJAJĄCYCH SIĘ GOSPODARKACH 76 PROC. PRACOWNIKÓW UMYSŁOWYCH UWAŻA, ŻE AI UCZYNI ICH PRACĘ ŁATWIEJSZĄ, A 75 PROC. TWIERDZI, ŻE BĘDZIE ONA BARDZIEJ INTERESUJĄCA

Również większość liderów biznesu dostrzega pozytywny wpływ AI na pracę. Aż 55 proc. pracowników umysłowych uważa, że AI otworzy przed nimi nowe możliwości zawodowe.

Zmiany nadchodzą. Zrozumiałe jest, że budzi to obawy wielu osób. Czy to jednak uzasadnione? Może lepiej przygotować się na nie i wykorzystać szansę na przekształcenie pracy i społeczeństwa? Jak zauważył Huang, możemy przecież skupić się na rozwoju umiejętności, które nadal będą niezastąpione, takich jak kreatywność, empatia czy zdolność do interakcji społecznych.

AUTOR
Klaudia Wojciechowska

Fundusze Europejskie odblokowane

W trakcie wizyty w Polsce Ursula von der Leyen, przewodnicząca Komisji Europejskiej, ogłosiła odblokowanie Funduszy Europejskich dla naszego kraju. To prawie 600 mld PLN z Polityki Spójności i Krajowego Planu Odbudowy. Pieniądze pozwolą pobudzić inwestycje oraz gospodarkę. Przeznaczone zostaną m.in. na zieloną i cyfrową transformację w gospodarce, zwiększenie bezpieczeństwa energetycznego dla ludzi i biznesu, innowacyjność i wykorzystanie nowoczesnych technologii.

– To efekt bardzo ciężkiej, wytężonej pracy całego rządu, na czele z premierem Donaldem Tuskiem, Ministerstwa Funduszy i Polityki Regionalnej i Ministra Sprawiedliwości. To także efekt ciężkiej, wytężonej pracy urzędników, którzy negocjowali bardzo trudne dokumenty i sporne kwestie z Komisją Europejską, tak aby te pieniądze mogły jak najszybciej trafić do Polaków i byśmy jak najszybciej mogli inwestować w Polsce środki z KPO i Funduszy Europejskich – przekonywał Jan Szyszko, wiceminister funduszy i polityki regionalnej.

W piątek 23 lutego Przewodnicząca Komisji Europejskiej Ursula von der Leyen odbyła wizytę w Polsce wraz z premierem Belgii Alexandrem De Croo. Oboje rozmawiali w jej trakcie z premierem Donaldem Tuskiem, a w trakcie wystąpienia dla mediów Ursula von der Leyen ogłosiła odblokowanie funduszy europejskich dla Polski.

– Te decyzje uwolnią do 137 mld euro dla Polski. Pochodzą z Funduszu Odbudowy i funduszy Polityki Spójności. Zostanie to zagwarantowane poprzez urząd Prokuratora Europejskiego. Jest to wspaniała wiadomość dla Europy i Polski – powiedziała Ursula von der Leyen, przewodnicząca Komisji Europejskiej.

Zgodnie z zapewnieniami Jana Szyszko odblokowanie funduszy to początek wytężonej pracy dla polskiego rządu. Celem jest wyrównanie szans rozwojowych w całym kraju.

– Dzisiaj kod pocztowy, pod którym mieszkamy, ma zbyt duże znaczenie i wpływ na jakość życia. Celem

inwestycji z Krajowego Planu Odbudowy i Funduszy Europejskich jest to, aby kod pocztowy był po prostu kodem pocztowym. By szanse były równe dla wszystkich mieszkańców Polski, niezależnie od tego, czy mieszkają w wielkim mieście, miasteczku czy na terenach wiejskich. Będziemy się o to starać przez najbliższe lata – powiedział Szyszko.

Wyrównywanie szans dzięki środkom z Polityki Spójności

Z Polityki Spójności na lata 2021-2027 Polska otrzyma rekordowe środki, bo ponad 340 mld PLN (76 mld euro). Najwięcej pośród państw Unii Europejskiej. Środki przeznaczone będą na wyrównanie szans rozwojowych między Polską a innymi państwami UE oraz rozwój wszystkich regionów kraju. Zostaną one rozdzielone na programy krajowe oraz regionalne.

Samorządy otrzymają około 150 mld PLN (33,5 mld euro). Pieniądze mają stać się impulsem rozwoju społeczno-gospodarczego regionów.

Pieniądze w ramach KPO

Krajowy Plan Odbudowy dla Polski to 55 inwestycji i 55 reform. Mają na celu wzmocnienie polskiej gospodarki po pandemii COVID-19, a także uczynienie jej bardziej odpornej na wszelkie kryzysy. Z KPO mamy otrzymać 59,8 mld euro (268 mld PLN). 25,27 mld euro (113,28 mld PLN) otrzymamy w postaci dotacji, a 34,54 mld euro (154,81 mld PLN) w formie preferencyjnych pożyczek.

Cele UE wskazują, że znaczną część budżetu będziemy musieli przeznaczyć na cele klimatyczne (46,6 proc.), ale również na transformację cyfrową (21,3 proc.) oraz na reformy socjalne (22,3 proc.).

ZGODNIE Z ZAPEWNIENIAMI JANA SZYSZKO ODBLOKOWANIE FUNDUSZY TO POCZĄTEK WYTĘŻONEJ PRACY DLA POLSKIEGO RZĄDU. CELEM JEST WYRÓWNANIE SZANS ROZWOJOWYCH W CAŁYM KRAJU

Samorządy otrzymają około 150 mld PLN (33,5 mld euro). Pieniądze mają stać się impulsem rozwoju społeczno-gospodarczego regionów.

KRAJOWY PLAN ODBUDOWY DLA POLSKI TO 55 INWESTYCJI I 55 REFORM. MAJĄ NA CELU WZMOCNIENIE POLSKIEJ GOSPODARKI PO PANDEMII COVID-19, A TAKŻE UCZYNIENIE JEJ BARDZIEJ ODPORNEJ NA WSZELKIE KRYZYSY. Z KPO MAMY OTRZYMAĆ 59,8 MLD EURO (268 MLD PLN)

W połowie grudnia Polska wysłała do Komisji Europejskiej pierwszy wniosek o płatność z Krajowego Planu Odbudowy. Zgoda Komisji Europejskiej na odblokowanie pierwszej wypłaty ma nastąpić do końca lutego. Potem przez miesiąc będzie trwało opiniowanie decyzji przez komitety Komisji.

Pieniądze z pierwszego wniosku o płatność z KPO pojawią się w kraju w kwietniu 2024 r. Ma to być ponad 6,3 mld euro (31 mld PLN), w tym dotacje to 2,7 mld euro a pożyczki – 3,6 mld euro.

Planowane jest złożenie kolejnych wniosków o środki z KPO w 2024 r. Pierwsze dwa mają pojawić się w połowie roku, a kolejna dwa pod jego koniec.

Niestety opóźnienia w realizacji KPO sprawiają, że polski rząd pracuje obecnie nad jego rewizją. Wstępny pakiet negocjacyjny ma być gotowy na początku marca 2024 r. Będzie poddany konsultacjom publicznym. Nowa wersja KPO ma być przekazana do Brukseli w kwietniu.

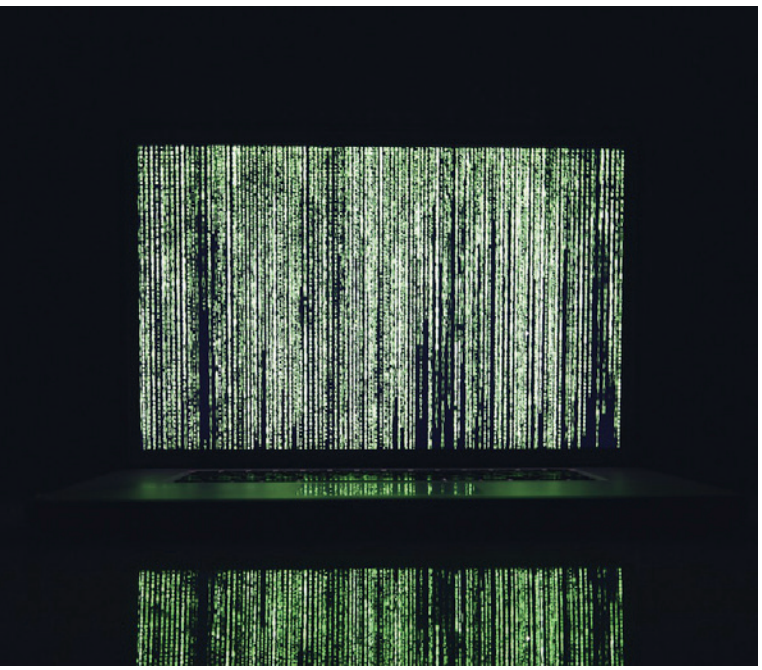
AUTOR
Michał Filipek

Wirtualizacja Proxmox – czynności po instalacyjne

Aby wygodnie zarządzać środowiskiem Proxmox z wykorzystaniem narzędzi SSH, podobnie jak dla większości maszyn z systemem operacyjnym Linux, sugerowane jest ustawienie dostępu do konsoli za pomocą kluczy SSH.

W pierwszym kroku należy wygenerować parę kluczy **prywatny/publiczny** na komputerze lokalnym, z którego planujemy zarządzać serwerem Proxmox.

ssh-keygen -t rsa -b 4096



Następnie klucz publiczny (**.pub**) należy przekopiować na serwer Proxmox do katalogu **/root/.ssh/authorized_keys**. Narzędziem ułatwiającym to zadanie jest ssh-copy-id, niestety nie jest ono wbudowane domyślnie w systemy operacyjne z rodziny Windows (obecne w systemach Linux, MacOS).

ssh-copy-id root@10.32.204.100

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'root@10.32.204.100'"
and check to make sure that only the key(s) you wanted were added.

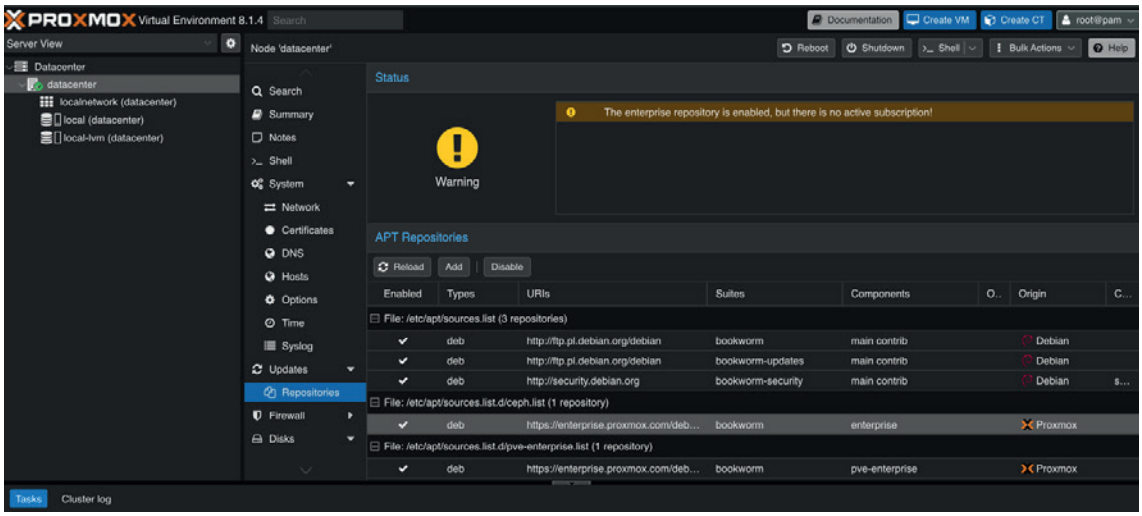
Jeżeli wszystko przebiegło poprawnie, przy kolejnej próbie logowania, nie będziemy pytani już o hasło.

ssh root@10.32.204.100

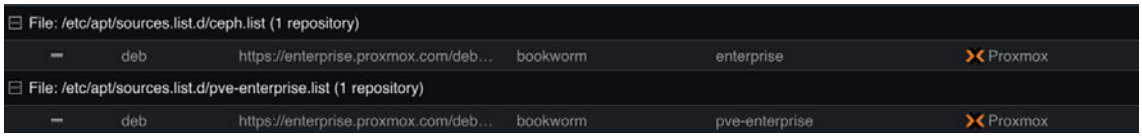
Aktualizacja systemu jednym z podstawowych zadań administracyjnych jest aktualizowanie systemu. Domyślna instalacja Proxmox zawiera repozytoria **enterprise**, które bez aktywowania subskrypcji uniemożliwiają pracę narzędzia **apt update**.

 # apt update
Get:1 http://security.debian.org bookworm-security InRelease [48.0 kB]
Err:2 https://enterprise.proxmox.com/debian/ceph-quincy bookworm InRelease
401 Unauthorized [IP: 212.224.123.70 443]
Err:3 https://enterprise.proxmox.com/debian/pve bookworm InRelease
401 Unauthorized [IP: 212.224.123.70 443]
Hit:4 http://ftp.pl.debian.org/debian bookworm InRelease
Get:5 http://ftp.pl.debian.org/debian bookworm-updates InRelease [55.4 kB]
Reading package lists... Done
E: Failed to fetch https://enterprise.proxmox.com/debian/ceph-quincy/dists/bookworm/InRelease 401 Unauthorized [IP: 212.224.123.70 443]
E: The repository 'https://enterprise.proxmox.com/debian/ceph-quincy bookworm InRelease' is not signed.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
E: Failed to fetch https://enterprise.proxmox.com/debian/pve/dists/bookworm/InRelease 401 Unauthorized [IP: 212.224.123.70 443]
E: The repository 'https://enterprise.proxmox.com/debian/pve bookworm InRelease' is not signed.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.

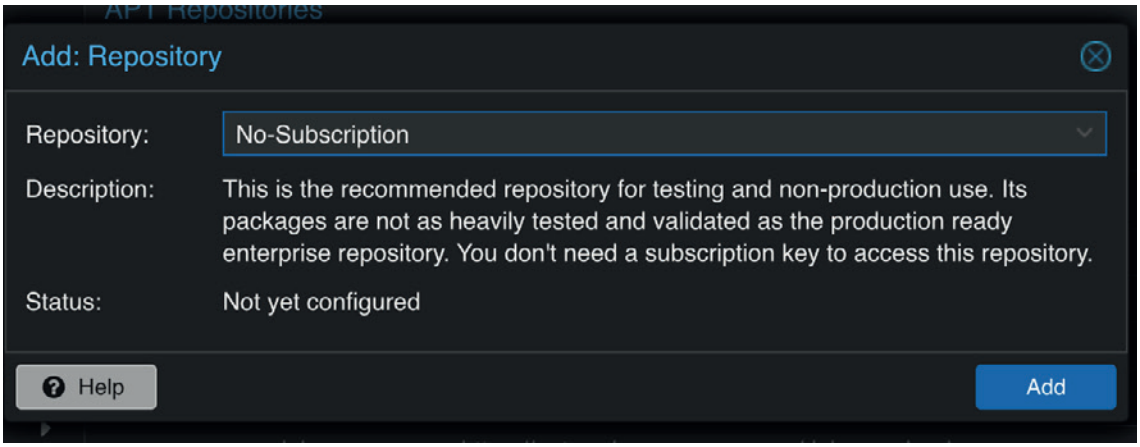
W celu weliminowania tego problemu należy wyłączyć repozytoria **enterprise**. Przechodzimy do sekcji Repositories



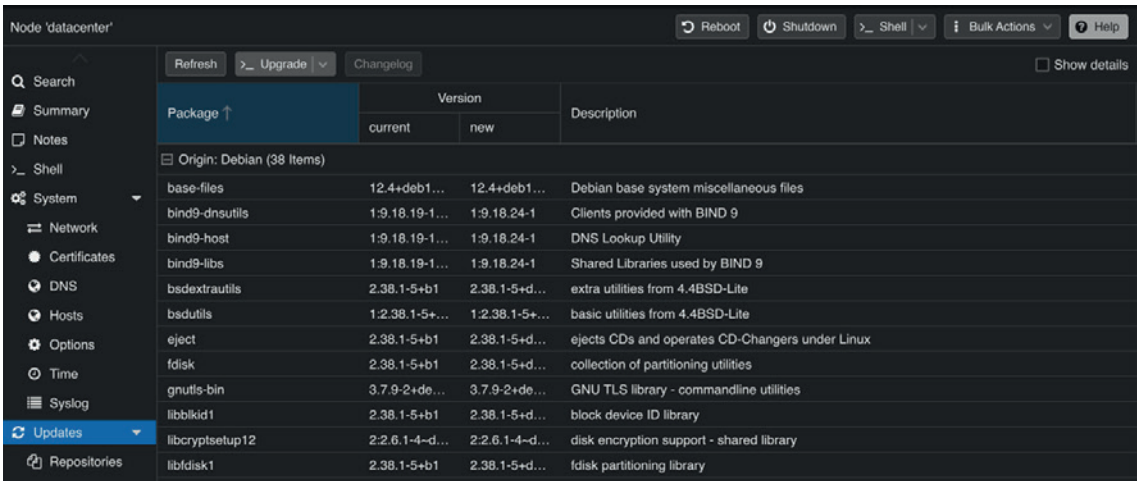
Zaznaczamy domyślne repozytoria Proxmox i klikamy **Disable**.



Teraz pozostaje dodanie repozytoriów **community**. Używamy opcji **Add**.

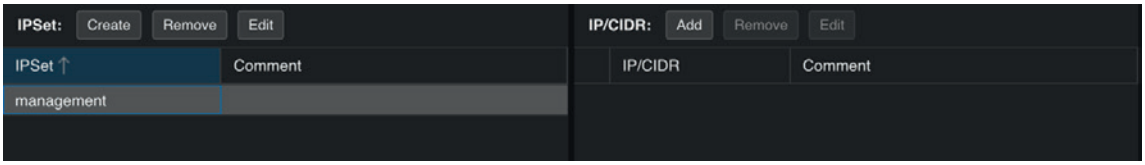


Jako ostatni krok wykonujemy update systemu.

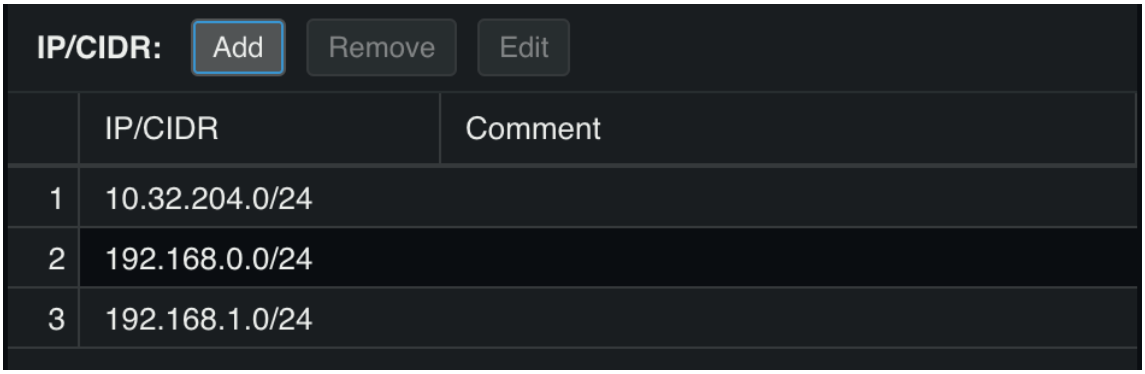


Można teraz wykonać reboot systemu.
reboot

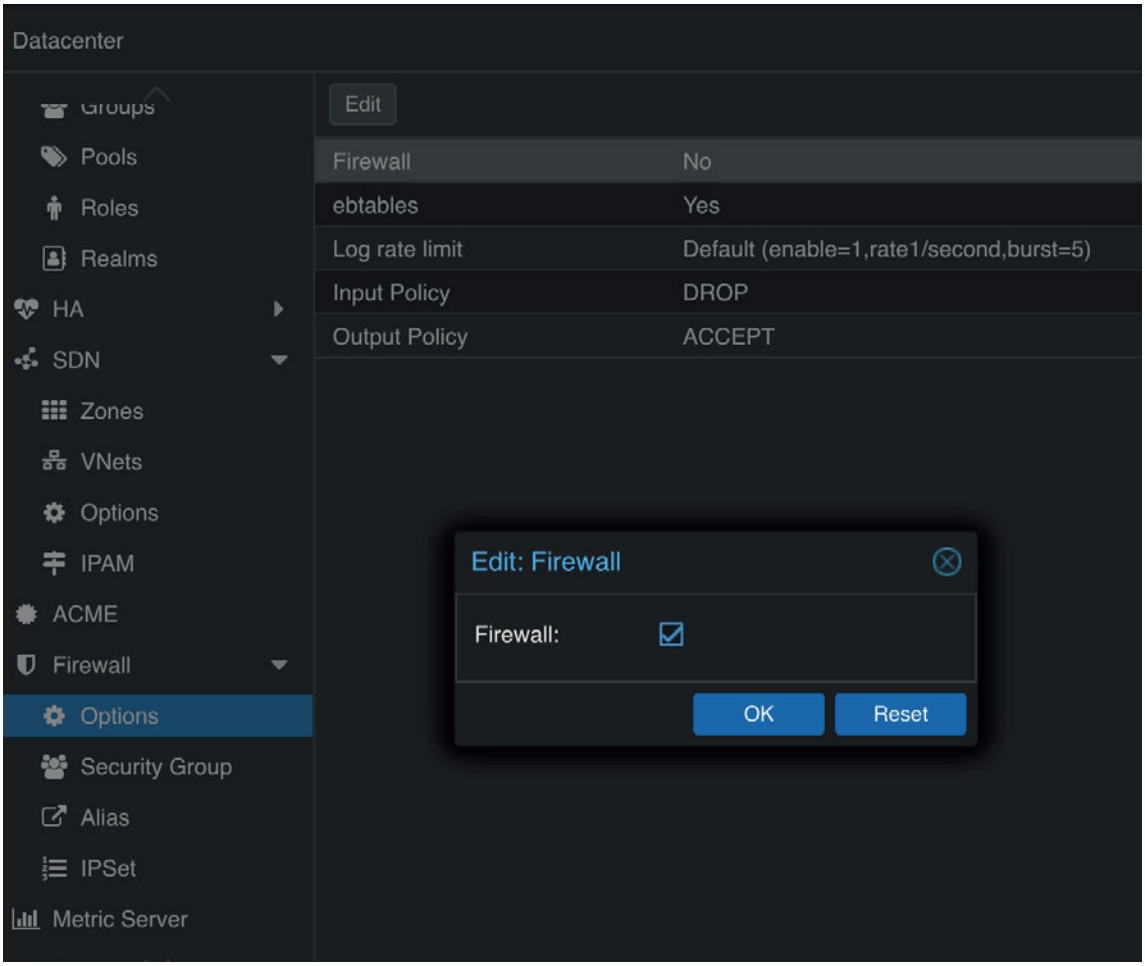
Podstawowy firewall bez względu na to, czy serwer Proxmox dostępny zainstalowany jest w środowisku z publicznym adresem IP, czy w dedykowanej sieci LAN, należy uruchomić firewall'a, dzięki któremu ograniczymy dostęp do zarządzania naszą platformą Proxmox. W tym celu przed włączeniem firewall'a należy dodać adresy ip/adresy podsieci, z którch zezwolony jest dostęp do Proxmox'a. W kolejnym kroku należy włączyć firewall'a. W sekcji **Firewall->IPSet** tworzymy listę **management** (Proxmox posiada wbudowne reguły firewall dla tak nazwanej listy)



Dodajemy adresy IP, adresy sieci, z jakich dostępny ma być panel zarządzania/ssh Proxmox.



Ostatecznie włączamy firewall w sekcji **Firewall->Options**.



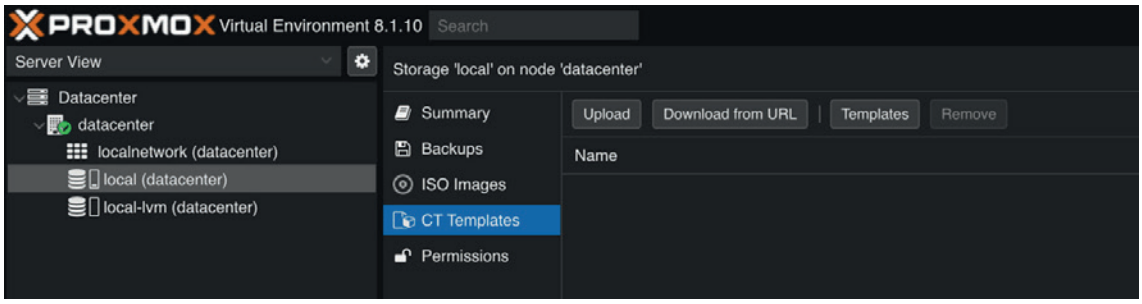
Uwagi:
Tak skonfigurowany firewall nie blokuje dostępu do maszyn wirtualnych, zabezpiecza jedynie dostęp do samego Proxmox'a.

Uruchamianie maszyn

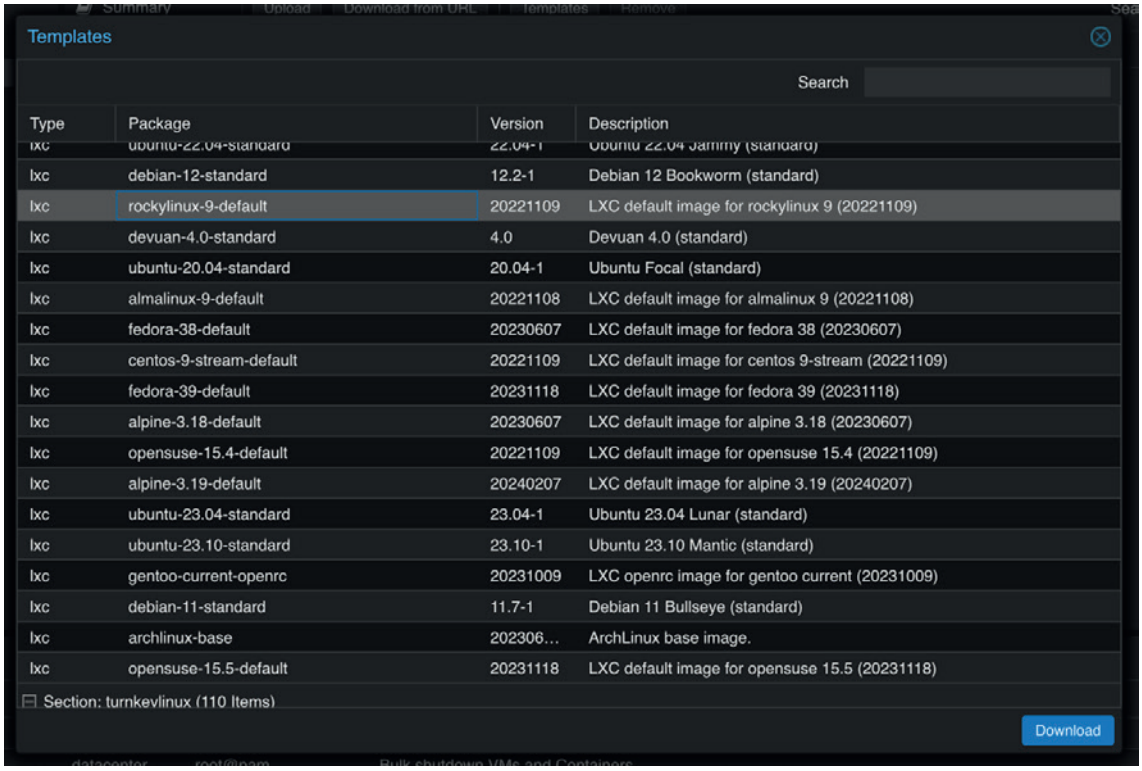
Aby zilustrować w jaki sposób uruchomić maszynę wirtualną na platformie Proxmox posłużymy się dwoma metodami, dzięki którym uruchomimy maszynę z systemem operacyjnym Linux. Każdy ze sposobów ma swoje plusy i minusy. Podstawowa różnica pomiędzy maszynami wirtualnymi, a kontenerami została omówiona w poprzednim artykule.

Instalacja kontenera LXC

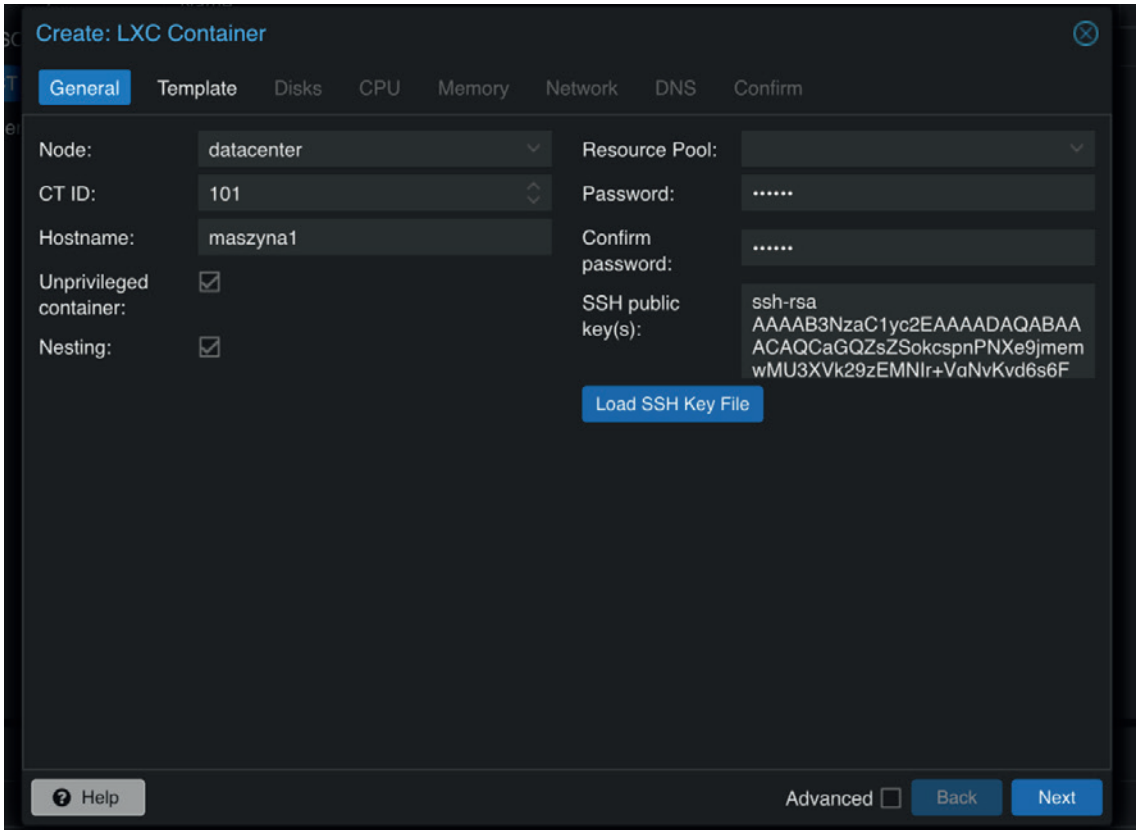
Wdrożenie kontenera LXC jest jednym z najszybszych sposobów uruchomienia systemu Linux w środowisku Proxmox. W pierwszym kroku należy pobrać interesujący nas szablon kontenera. Oczywiście, jest też możliwość upload'u naszego własnego szablonu. W przykładzie posłużymy się gotowym szablonem systemu Rocky Linux.



W sekcji Templates wybieramy rockylinux-9-default I zaznaczamy **Download**.



Od teraz szablon jest już dostępny w systemie Proxmox i można na jego podstawie tworzyć kontenery. Zaznaczmy **Create CT** w prawym górnym rogu ekranu.



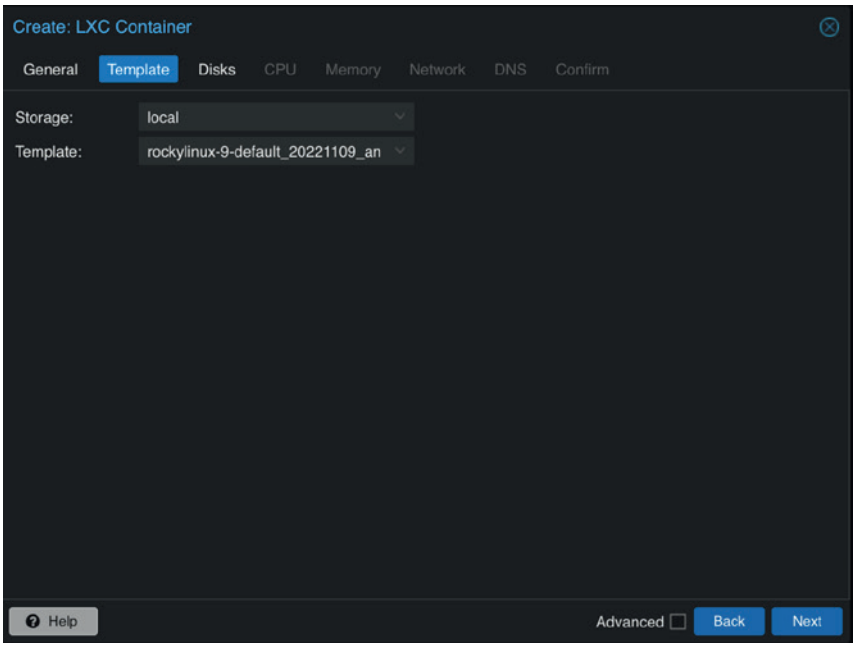
Ustawiamy:

CT ID (unikalny identyfikator maszyny nadawany automatycznie lub ręcznie)

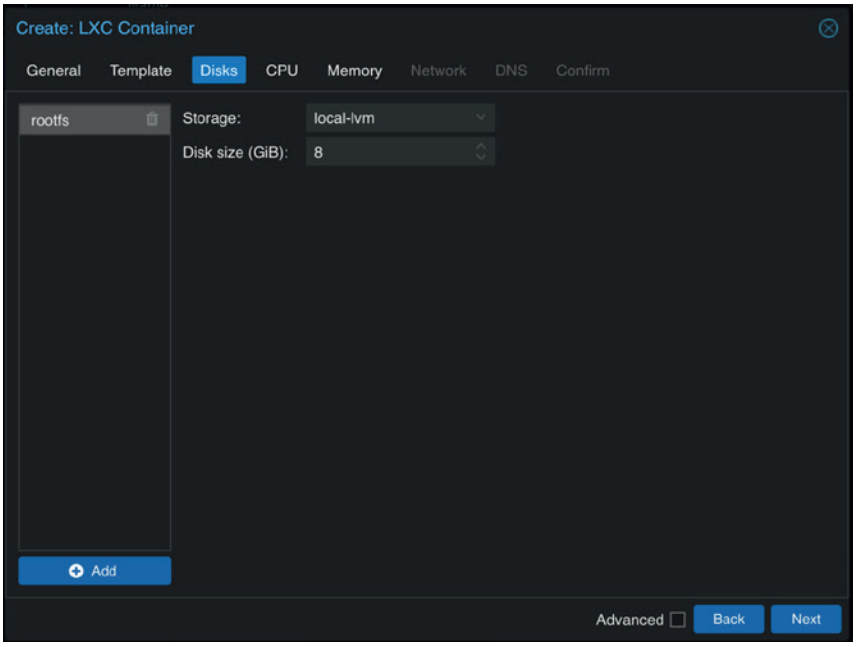
Hostname (nazwę dla naszej maszyny), Password (hasło dla użytkownika)

SSH public key (tutaj możemy podać wcześniej wygenerowany klucz publiczny)

Next, wskazujemy **Template** z jakiego utworzymy maszynę.

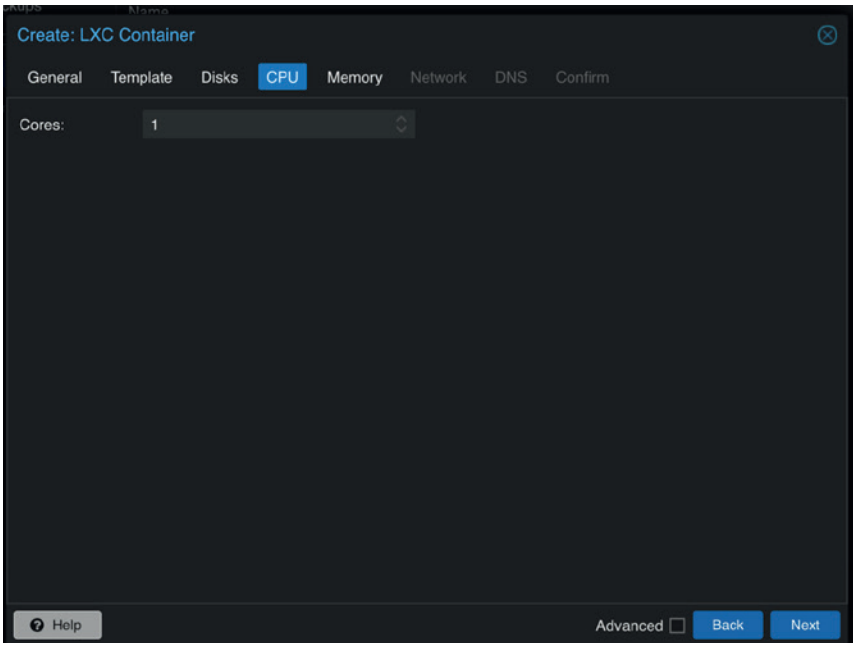


Ustawienia rozmiaru pamięci dyskowej. Warto tutaj wspomnieć, iż w wyniku domyślnej instalacji Proxmox dysponujemy jedynie opcją local-lvm, jest to grupa volumenów, na której, dla każdej z maszyn, utworzony zostanie volumen logiczny stanowiący jej dysk. W kolejnych artykułach przybliżymy różnice pomiędzy różnymi typami obsługiwanych magazynów danych z podziałem na magazyny plikowe oraz blokowe.



Przydzielenie zasobów CPU

W przypadku kontenerów LXC mamy jedynie możliwość określenia ilości rdzeni procesora/limitów. Nie mamy tutaj, typowej dla większości wirtualizatorów, emulacji procesora i związanych z nią dodatkowych ustawień. Wspomniane menu dla maszyn wirtualnych jest zdecydowanie bardziej rozbudowane.

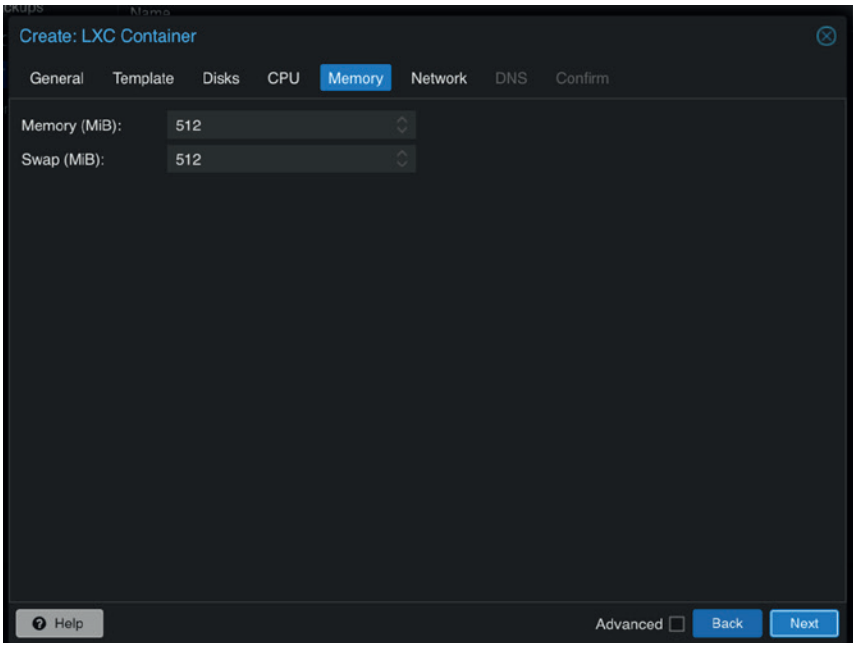


Rozmiar pamięci RAM

Zarządzanie pamięcią RAM jest istotne dla zapewnienia odpowiedniej wydajności i stabilności wirtualnych maszyn i kontenerów, jak również dla efektywnego wykorzystania zasobów fizycznego serwera.

Memory ilość pamięci RAM przydzieloną do kontenera LXC.

SWAP ustawienia dotyczące pamięci wirtualnej (swap), która służy jako bufor dla chwilowych deficytów pamięci RAM (wykorzystywany jest dysk twardy).



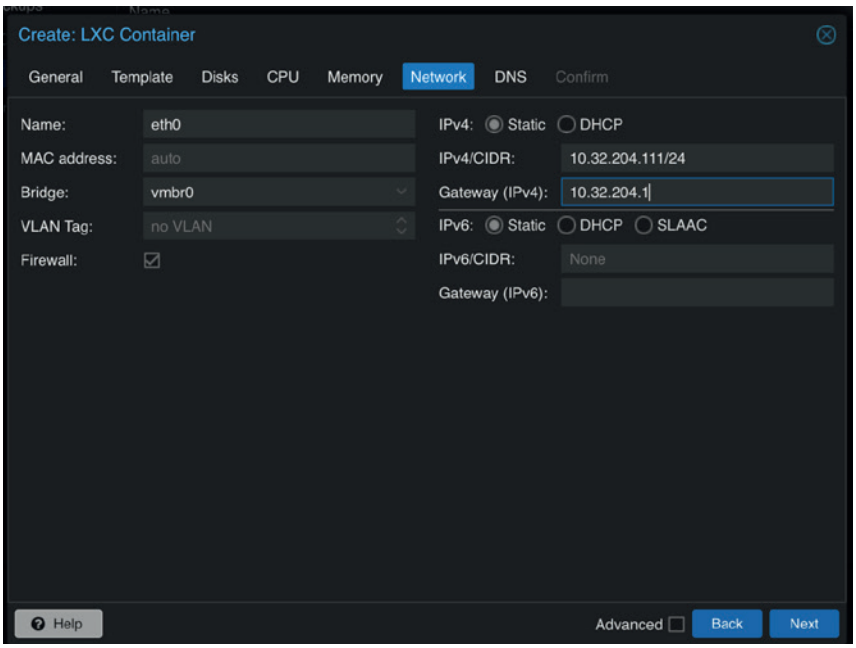
Ustawienia sieci

Proxmox posiada duże możliwości w zakresie konfiguracji sieci dla maszyn wirtualnych i kontenerów. Do najpopularniejszych typów sieci należą:

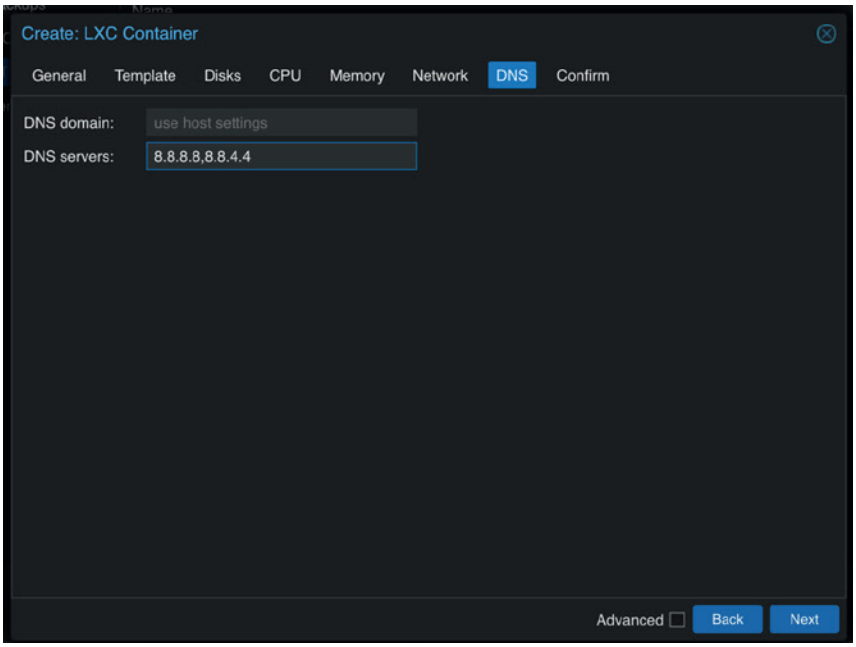
Most sieciowy (bridge) Domyślnie, Proxmox konfiguruje most sieciowy o nazwie vmbr0. Jest to wirtualny interfejs, który pozwala maszynom wirtualnym i kontenerom na udostępnianie fizycznego interfejsu sieciowego serwera. vmbr0 jest zazwyczaj przypisany do pierwszego aktywnego interfejsu sieciowego na hoście i używa tego interfejsu do komunikacji z siecią.

Route odnosi się do konfiguracji sieciowej, gdzie ruch z maszyn wirtualnych lub kontenerów jest kierowany (routowany) przez hosta Proxmox do reszty sieci, bez wykorzystania mostu sieciowego (bridge). Taka konfiguracja umożliwia bardziej szczegółowe kontrolowanie ruchu sieciowego i może być przydatna w bardziej złożonych środowiskach sieciowych.

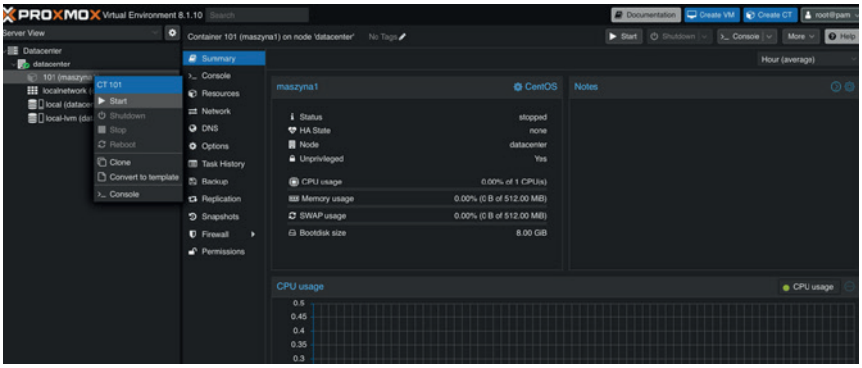
W naszym przykładzie użyjemy sieci typu **bridge**.



Wskazanie serwerów DNS z jakich korzystać będzie kontener LXC

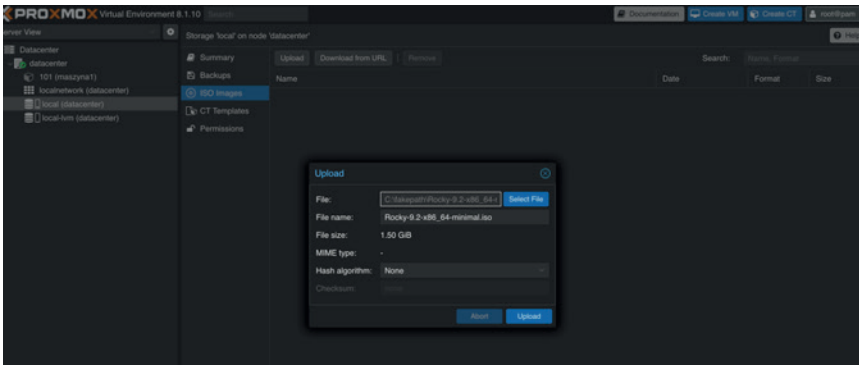


Ostatni krok to wystartowanie kontenera.

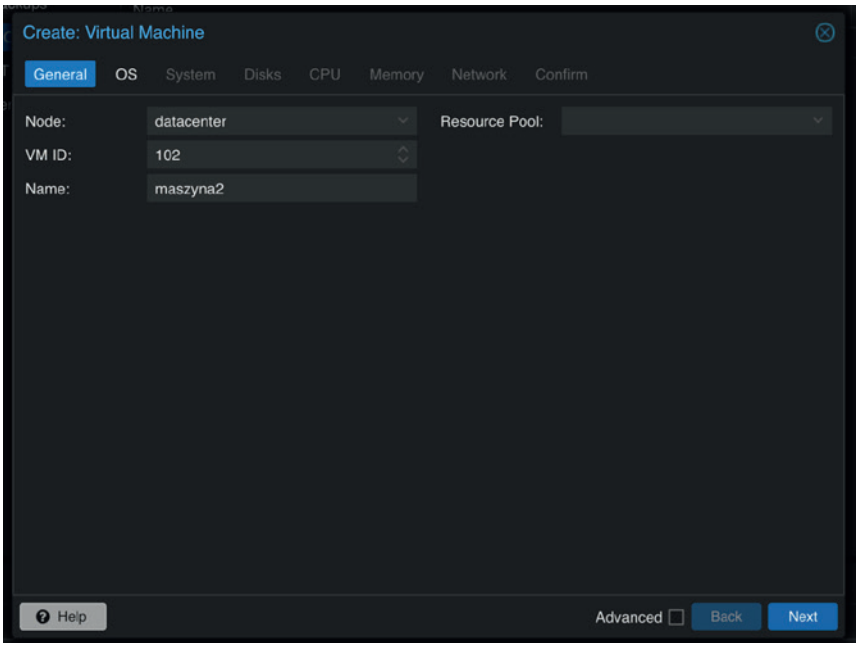


Instalacja maszyny z obrazu ISO

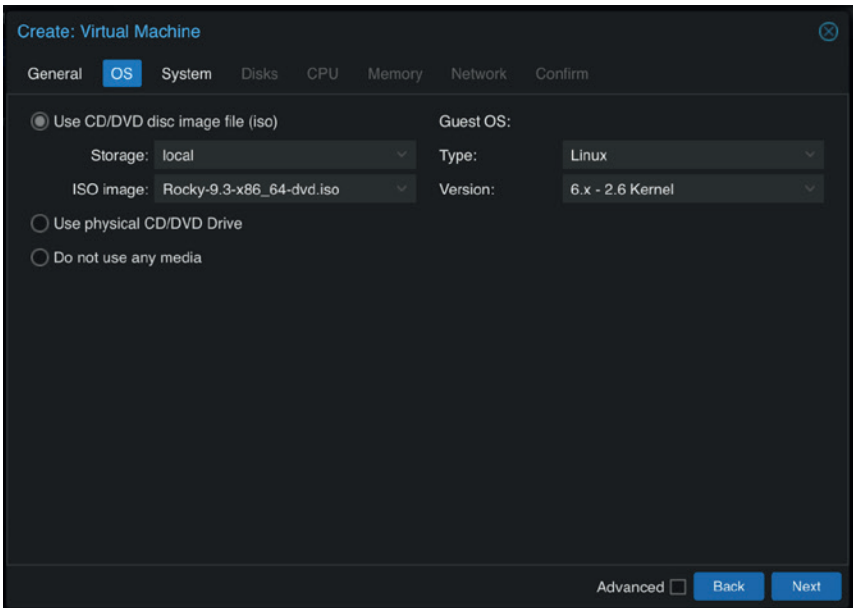
Najbardziej popularną metodą uruchomienia maszyny wirtualnej jest zainstalowanie jej z obrazu ISO. Wybrany przez nas obraz ISO należy zaimportować do Proxmox.



W górnym rogu klikamy **Create VM**.

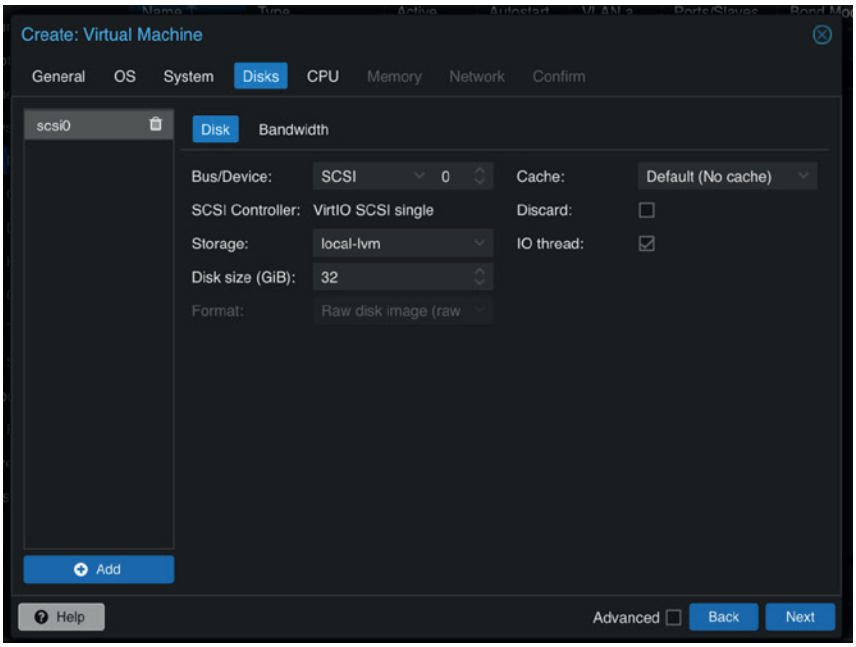


Wybieramy obraz ISO, z jakiego będziemy instalować naszą maszynę.



Dysk

Najbardziej wydajną wersją kontrolera dysku jest VIRTIO. Systemy z rodziny linux mają wbudowaną obsługę (sterownik) dla tego typu emulowanego dysku. Dla maszyn z windowsem rekomenduje się doinstalowanie takiego sterownika.



CPU

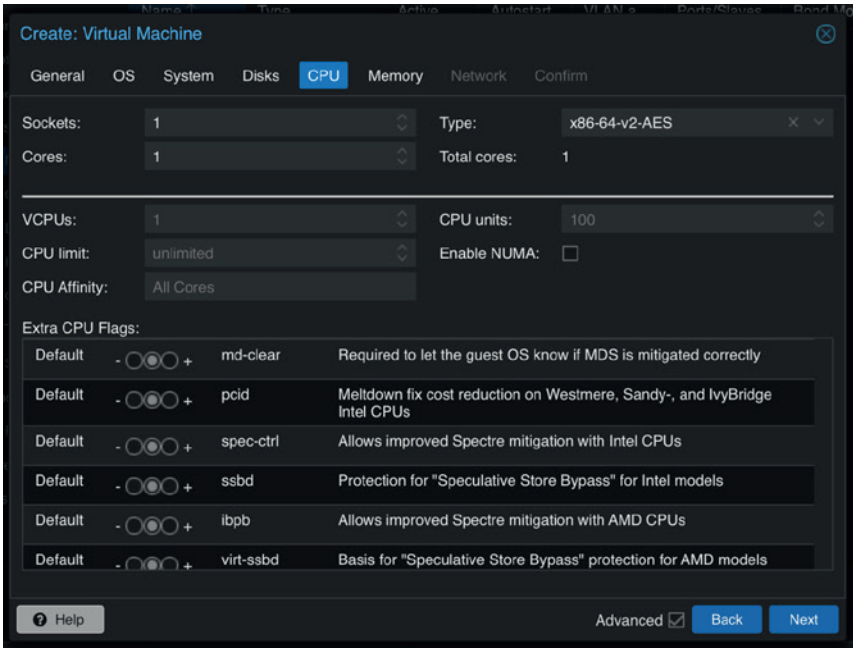
Sekcja CPU służy do konfiguracji ustawień procesora (CPU) dla maszyn wirtualnych (VM). Oto główne funkcje i zastosowania tej sekcji:

Przypisywanie zasobów CPU: W sekcji CPU możesz określić, ile rdzeni procesora będzie przypisanych do konkretnej maszyny wirtualnej. Pozwala to na optymalne wykorzystanie zasobów serwera przez rozdzielenie mocy obliczeniowej pomiędzy poszczególne VM.

Typ i model procesora: Możesz wybrać typ oraz model procesora, jaki ma być symulowany dla maszyn wirtualnych. Daje to możliwość emulacji określonych funkcji CPU, co może być ważne dla kompatybilności lub wydajności określonych aplikacji.

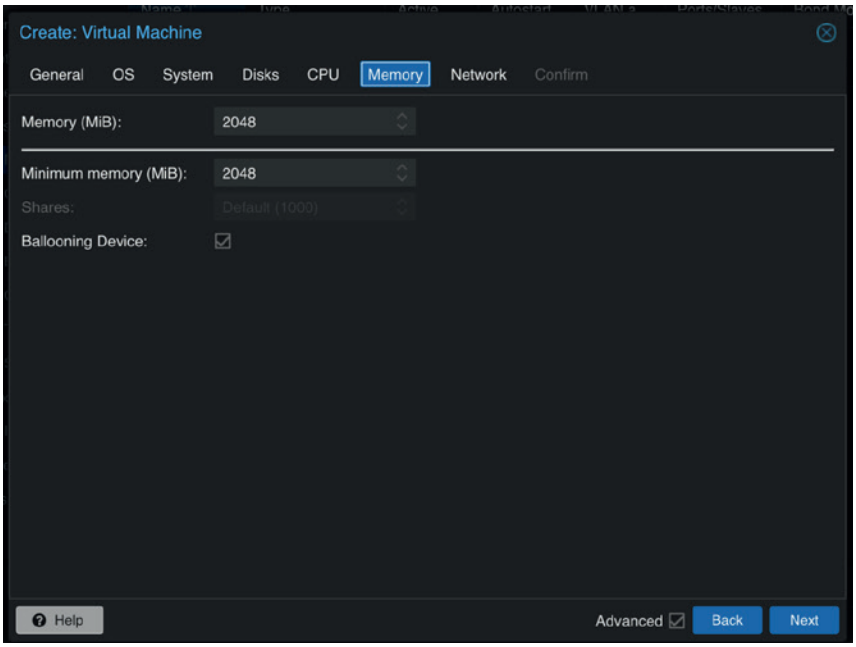
Priorytetowanie: Można ustawić priorytety dla poszczególnych VM, co określa, jak ważne jest przydzielanie im zasobów CPU w stosunku do innych instancji.

Konfiguracja NUMA (Non-Uniform Memory Access): Jeśli serwer posiada konfigurację NUMA, można zarządzać przypisaniem CPU w kontekście lokalności pamięci, co może znacząco wpłynąć na wydajność.



Pamięć RAM

Poza przydzieleniem pamięci RAM dla maszyny wirtualnej można także skorzystać z mechanizmu Ballooning (na systemach Windows konieczne jest doinstalowanie sterownika). Balonowanie pamięci (Memory Ballooning): Jest to technika, która pozwala na dynamiczną realokację pamięci RAM między maszynami wirtualnymi na tym samym fizycznym serwerze. Jeśli maszyna wirtualna używa mniej pamięci niż jej przydzielono, nadwyżka może być tymczasowo przydzielona innym VM, które mają większe potrzeby.



Po wystartowaniu maszyny, w sekcji Console dostaniemy następujący ekran powitany.

Teraz pozostaje przejść proces instalacji systemu, zgodnie z kreatorem dostępnym w danej dystrybucji Linux i na koniec zrestartowanie maszyny wirtualnej.

Podsumowanie

Przedstawione metody tworzenia maszyn wirtualnych nie wyczerpują tematu i stanowią jedynie wstęp do tego zagadnienia. Inne, popularne metody uruchamiania maszyn w środowiskach wirtualnych polegają na zaimportowaniu obrazu (**cloud image**) interesującej nas dystrybucji Linux i uruchomienie go z wykorzystaniem mechanizmu **cloud-init** (mechanizm wstępnej konfiguracji).

LOKALNI

Wyszukiwarka dla małych i średnich operatorów

Daj się znaleźć w internecie i dołącz do Lokalnych

sklep.misot.pl/lokalni

ISP Forum

Ogólnopolskie forum Małych i Średnich Operatorów Telekomunikacyjnych

ISPFORUM.PL