



ISPROFESSIONAL

ISSN: 2449-5581

#7 (MAJ 2024)

STR. 9
EKSPANSJA SZTUCZNEJ
INTELIGENCJI

STR. 20
ZJAZD W JANOWIE
PODLASKIM - RELACJA

STR. 25
CÓŻ TAM, PANIE,
W TELEWIZJI?

STR. 29
PODWYŻKA OPŁATY
TELEKOMUNIKACYJNEJ

STR. 39
GOOGLE WYBIERZE
ZA CIEBIE

generacja

STR. 6

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. Powstał, 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

Drodzy Czytelnicy,

W najnowszym wydaniu ISProfessional pragniemy skupić się na temacie, który dynamicznie zmienia oblicze wielu branż, w tym także telekomunikacji – mowa o sztucznej inteligencji (AI). Dla małych i średnich operatorów telekomunikacyjnych AI nie jest już tylko odległą koncepcją czy przedmiotem dyskusji akademickich. Stała się rzeczywistością, która przynosi konkretne korzyści, stawia nowe wyzwania i otwiera przed nami fascynujące możliwości.

Przyglądamy się, jak małe i średnie przedsiębiorstwa telekomunikacyjne mogą wykorzystać AI do optymalizacji swoich operacji, poprawy jakości usług oraz zwiększenia satysfakcji klientów. Omawiamy także, w jaki sposób sztuczna inteligencja może wspierać te firmy w przewidywaniu trendów rynkowych, zarządzaniu sieciami oraz w walce z cyberzagroženiami, które stały się częścią cyfrowej codzienności.

Nie pomijamy również wyzwań, jakie niesie ze sobą implementacja AI. Omawiamy aspekty

etyczne, techniczne oraz finansowe, z którymi małe i średnie firmy mogą się zmierzyć, decydując się na integrację rozwiązań opartych na sztucznej inteligencji. Naszym celem jest dostarczenie praktycznej wiedzy, która pomoże naszym czytelnikom podejmować świadome decyzje i kształtować przyszłość ich przedsiębiorstw w harmonii z najnowszymi trendami technologicznymi.

Zachęcamy do lektury artykułów przygotowanych przez ekspertów z branży telekomunikacyjnej oraz specjalistów z dziedziny AI. Mamy nadzieję, że treści zawarte w tym wydaniu zainspirują Państwa do eksplorowania możliwości, jakie oferuje sztuczna inteligencja. Będą one stanowić wartościowy wkład w rozwój Państwa firm.

Zyczymy przyjemnej lektury!
Redakcja ISProfessional

Kontakt z redakcją:
prasa@misot.pl

Nr w rejestrze wydawnictwo:
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 Koścička

Współpraca:
Paweł Białas
Łukasz Biernacki
Aleksandra Czerech
Krzysztof Czuszek
Michał Filippek
Sebastian Kachel
Adam Kossowski
Krzysztof Kołodziej
Maciej Linscheid
Marcin Pilak
Piotr Wasyk
Marcin Zemła

Projekt ISProfessional #7 (maj 2024) wydany w maju 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.

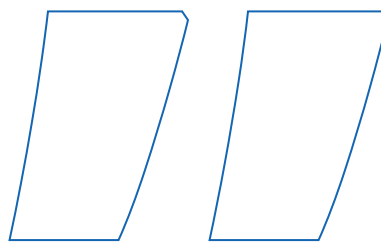
Informacje na Państwa temat posiadamy z publicznie dostępnego źródła – Rejestru przedsiębiorców telekomunikacyjnych. Dane, jakie posiadamy i przetwarzamy to imię, nazwisko, nazwa firmy, adres firmy, NIP, KRS, adres e-mail. Mają Państwo możliwość zażądania, aby nie otrzymywać więcej takich informacji.

Określone powyżej informacje na Państwa temat posiadamy po to, by wysłać 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 wysłać 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 przechowywanych 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 nieciekawe. Mogą Państwo także złożyć skargę w Urzędzie Ochrony Danych Osobowych pod adresem ul. Stawki 2, 00-193 Warszawa.



Spis treści

AI	
GenAI – genialne oszustwo	6
Ekspansja sztucznej inteligencji.....	9
Rewolucja w kreacji wideo	11
AI w złych rękach	13
ENERGIA	
Jak sztuczna inteligencja wpłynie na energetykę?.....	17
Z ŻYCIA MIŚOT	
Zjazd MiŚOT w Janowie Podlaskim – relacja	20
TELEWIZJA	
Cóż tam, panie, w telewizji?	25
PRAWO I TELEKOMUNIKACJA	
Podwyżka opłaty telekomunikacyjnej.....	29
Z PAMIĘTNIKA BEZPIECZNIKA	
NIS 2, czyli ja się chyba powieszę	31
ZARZĄDZANIE	
IP Scan w Polsce. MiŚOT-y mogą sprawdzić ochronę swoich własności intelektualnych	37
TRENDY	
Google wybierze za ciebie	39
FELIETON	
Sztuczna inteligencja: od inspiracji do odpowiedzialności	41
BAZA WIEDZY	
Wirtualizacja Proxmox – typy magazynów danych.....	43

Produkty marki **cudy**



Nowoczesne rozwiązania sieciowe dla domu i biura

Technologia
Wi-Fi6



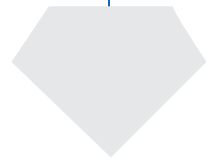
Transmisja
2.5Gbps

Superszybkie Wi-Fi
AX3000



Tryb CCTV/VLAN
zasięg do 250m

Do 30W
na port PoE+



AI

AUTOR

Krzysztof Kołodziej

GenAI – genialne oszustwo

Prawdopodobnie nie zdajemy sobie nawet sprawy, jak bardzo sztuczna inteligencja jest już wykorzystywana w otaczającym nas świecie mediów i jak łatwo możemy zostać zmanipulowani.

Spośród narzędzi GenAI (ang. generative artificial intelligence, czyli generatywnej sztucznej inteligencji), największą popularnością cieszy się ChatGPT, który już na co dzień pomaga dzieciom odrabiać zadania domowe, a rodzicom tworzyć prezentacje multimedialne. To jednak tylko wierzchołek góry lodowej możliwości, jakie daje nam uczenie maszynowe, na którym opiera się GenAI. Jeśli więc mamy wrażenie, że szerokie zastosowania dla niej to daleka przyszłość, to jesteśmy w grubym błędzie.

W świecie mediów działa już wiele zaawansowanych narzędzi GenAI. Netflix wykorzystuje je do analizowania preferencji i personalizowania nowych treści, zwiększając naszą

satisfakcję nawet o 30%. Programy do edycji video mogą zwiększyć swoją efektywność o 40 proc., co przyspiesza proces produkcji bez straty jakości, a GenAI na YouTube podsuwa nam reklamy, którymi jesteśmy bardziej zainteresowani, co daje większą klikalność.

Stare, klasyczne filmy są rewitalizowane i zyskują wyższą rozdzielczość, a wirtualne plany zdjęciowe i rozszerzona rzeczywistość AR (Augmented Reality) pomagają BBC realizować unikalne produkcje telewizyjne.

Radiowy głos AI

W Polsce zadebiutowała już prezenterka radiowa AI Basia, która latem 2023 prowadziła audycje w Radiu



Piekary. Audycje były w całości generowane i prowadzone przez AI. Co ciekawe premiera odbyła się 22 lipca, w Światowy Dzień Mózgu. Czy traktować to jako wyzwanie? Czy słuchacze, którzy przypadkiem trafili na te audycje, wiedzieli, że nie prowadzi ich DJ z krwi i kości?

Jeśli sami chcecie zbudować takie radio, podaję krótki przepis, z jakich narzędzi można skorzystać: Midjourney (generator grafiki), ElevenLabs (rozwiązanie Generative Voice AI zamieniające tekst na mowę oraz ChatGPT (model językowy firmy OpenAI).

Sky(net) **is the limit**

Radio jest ciekawym eksperymentem, ale prawdziwym wyzwaniem dla GenAI jest produkcja video. Jak się okazuje nawet w Polsce mamy już za sobą premierę reklamy telewizyjnej środka na erekcję w całości wygenerowanej przez AI. Agencja, która ją stworzyła twierdzi, że zdecydowanie obniżyła koszty w porównaniu z innymi podobnymi produkcjami. Od zastąpienia ludzi awatarami w reklamie jest już tylko krok do zastąpienia aktorów w produkcjach filmowych albo prezenterów i dziennikarzy w kanałach telewizyjnych.

Tworzy się właśnie ciekawy projekt informacyjnej stacji telewizyjnej pod nazwą Channel 1. Na razie zadebiutuje jako 30- minutowa produkcja dostępna poprzez FAST channel raz w tygodniu. Ambicją twórców jest tworzenie serwisu informacyjnego dla każdego użytkownika. Wyzwaniem jest stworzenie kanału, w którym nie będziemy w stanie odróżnić oglądania awatarów sztucznej inteligencji od człowieka. Najciekawszym pomysłem jest jednak odtwarzanie wydarzeń, których nie zarejestrowały kamery. Będą to na przykład wizualizacje procesów sądowych zamkniętych dla kamer. Do tej pory w takich sytuacjach korzystaliśmy z rysowników. Teraz rzeczywistość będzie odtwarzana jako relacja z miejsca zdarzenia.

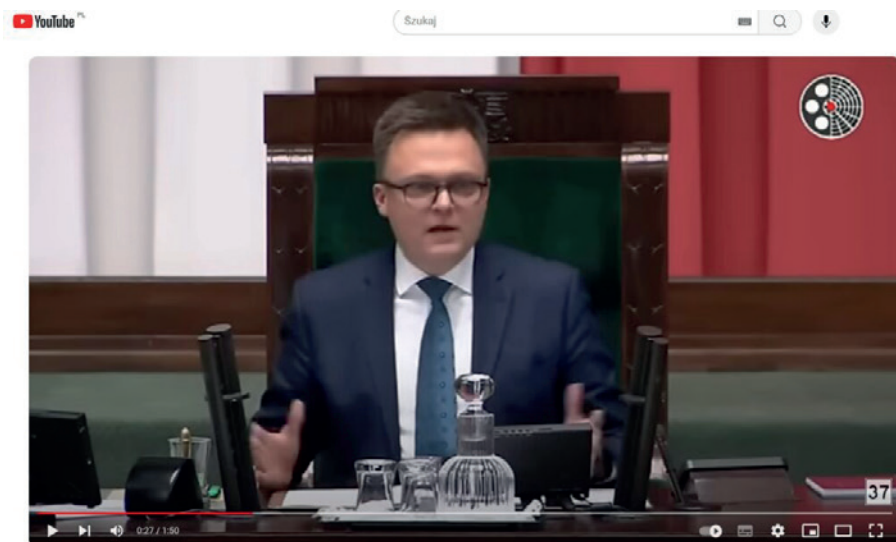


NAWET W POLSCE MAMY JUŻ ZA SOBĄ PREMIERĘ REKLAMY TELEWIZYJNEJ ŚRODKA NA EREKCJĘ W CAŁOŚCI WYGENEROWANEJ PRZEZ AI. AGENCJA, KTÓRA JĄ STWORZYŁA TWIERDZI, ŻE ZDECYDOWANIE OBNIŻYŁA KOSZTY

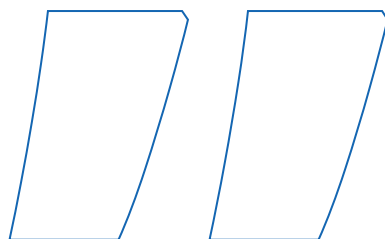
Autorzy zastrzegają, że informacje będą pozyskiwać bardzo rzetelnie z wiarygodnych źródeł i nie będą kreować nowej rzeczywistości. Pytanie brzmi, w jaki sposób my widzowie będziemy w stanie to zweryfikować?

Czy uratuje nas AI Act?

Jesteśmy już tylko o krok od bardzo niebezpiecznego narzędzia manipulacji zwanego deepfake. Z pomocą przychodzi nam Parlament Europejski, który w grudniu 2023 przyjął europejską ustawę o sztucznej inteligencji



Hołownia Patostreamer - przeróbka AI - Posiedzenie Sejmu.



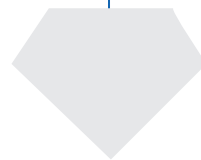
BADANIA RYNKU USA WSKAZUJĄ, ŻE CO DRUGI DOROSŁY AMERYKANIN OBAWIA SIĘ SZTUCZNEJ INTELIGENCJI I JEJ WPŁYWU NA SPOŁECZEŃSTWO

(tzw. AI Act). Klasyfikuje ona poziomy ryzyka różnych modeli, zakazuje korzystania ze sztucznej inteligencji w niektórych przypadkach i analizuje potencjalny wpływ AI na prawa człowieka.

Mimo że jest to pierwsza na świecie taka regulacja, niestety jakoś nie czuję się jeszcze szczególnie chroniony, zwłaszcza że wystarczy krótka instrukcja z Youtube i mogę w kilka minut wygenerować własnego deepfake'a, a bohaterami wielu takich produkcji stają się ostatnio nasi politycy, szczególnie zaś Szymon Hołownia.

W swoich obawach nie jestem odosobniony. Badania rynku USA wskazują, że co drugi dorosły Amerykanin obawia się sztucznej inteligencji i jej wpływu na społeczeństwo. Polacy, według najnowszego raportu Deloitte, boją się AI, ale głównie w aspekcie utraty pracy, czy słusznie? Kwestię tę rozważał niedawno na naszym portalu Michał Koch.

Przed nami w Polsce wybory samorządowe, do parlamentu europejskiego, a w przyszłym roku prezydenckie. Za wschodnią granicą wojna. Czy nie powinniśmy się czuć zagrożeni dezinformacją i manipulacją wysokiej jakości, opartą na wysokiej technologii GenAI? Czy jesteśmy zabezpieczeni przed zalewem dipfejków?



AI

AUTOR

Marek Nowak

Ekspansja sztucznej inteligencji

Te dane mogą zaskakiwać. Globalne wydatki na technologie cyfrowe na koniec bieżącego roku będą aż siedem razy większe niż tempo wzrostu gospodarczego. Rośnie też liczba firm i organizacji, które korzystają i planują korzystać ze sztucznej inteligencji. Ta technologia wdziera się już właściwie do każdej dziedziny działalności przedsiębiorstw. Także do lodówek.

Opinie menedżerów w Europie, na Bliskim Wschodzie i w Afryce dotyczące sztucznej inteligencji i inwestycji w technologie są jednoznaczne. Boom wokół GenAI (generatywnej sztucznej inteligencji), który obserwowaliśmy w trakcie ostatniego roku, wpłynął na zmianę spojrzenia przedsiębiorstw na możliwości oferowane przez narzędzia

wykorzystujące tę technologię. Warto także zwrócić uwagę na fakt, że jest to rewolucja, w której polskie przedsiębiorstwa uczestniczą na równych prawach, jak inne państwa Europy.

Duże pieniądze

W 2023 r. na rozwiązania GenAI wydano łącznie 19,4 mld dolarów. Według prognoz firmy doradczej IDC, w perspektywie trzech najbliższych lat inwestycje te osiągną jednak dużo większe wartości. Globalnie będzie to wartość sięgająca 150 mld dolarów. Dane wskazują też, że aż 30 proc. inwestycji w AI do 2027 roku będą stanowiły wydatki na jej generatywną odmianę.

– Widzimy ogromną zmianę. Mimo niestabilnej sytuacji geopolitycznej, inwestycje w technologie cyfrowe będą rosły w 2024 r. aż siedem razy szybciej niż cała gospodarka. Kluczową rolę będzie odgrywała oczywiście sztuczna inteligencja, która będzie wdrażana w niemal każdym obszarze działalności przedsiębiorstw. Jeśli w samym tylko regionie EMEA budżet na AI wzrośnie w przyszłym roku o 40 proc., oznacza to dodatkowe 30 mld dolarów wydatków na technologie. To najlepiej pokazuje skalę i tempo zmian – zauważa Ewa Zborowska, research director z IDC Polska.

Firmy nie zwiększają przy tym inwestycji w technologie tylko dlatego, że na AI jest moda, ale dlatego, że mogą na tym zarobić. Wdrożenie tej technologii może przynieść zwiększenie efektywności pracy, obniżenie kosztów i zdobycie nowych źródeł przychodów.



– Dzięki technologii AI pojawią się nowe możliwości, których dzisiaj nie ma – dodaje Ewa Zborowska.

IDC szacuje, że do 2026 r. aż 70 proc. dużych firm w regionie EMEA zacznie wykorzystywać sztuczną inteligencję do podejmowania decyzji biznesowych w czasie rzeczywistym. Połowa z nich będzie korzystać z GenAI jako wsparcia w projektowaniu nowych produktów i usług, co dwukrotnie skróci czas ich wprowadzania na rynek.

– Przedsiębiorstwa uczestniczą w technologicznym wyścigu nie tylko dlatego, że pierwszeństwo daje im rynkową przewagę. Te firmy, które tego nie zrobią, mogą w perspektywie 5 lat zacząć tracić swoje udziały rynkowe – tłumaczy Ewa Zborowska.

Wszędzie AI

Częścią tej technologicznej rewolucji są także konsumenci i pracownicy.

– Rozpoczynamy nowy rozdział. Żyjemy obecnie w erze AI Everywhere, w której sztuczna inteligencja jest nie tylko łatwo dostępna, ale przede wszystkim staje się integralną częścią strategii oraz działań biznesowych. Przekłada się to również na życie społeczeństwa. W regionie EMEA do 2026 r. 75 proc. organizacji rozważy wykorzystanie AI lub już z tej technologii korzysta. Ma to wpływ na zwykłych obywateli. Dużą popularnością wśród użytkowników cieszą się przede wszystkim generatywne formy AI. Z GenAI za dwa lata będzie korzystało aż 85 proc. mieszkańców Europy, Bliskiego Wschodu i Afryki – uważa Ewa Zborowska.

Eksperti IDC podkreślają, że do 2025 r. już 45 proc. dużych firm w regionie EMEA będzie wykorzystywać GenAI do przyspieszenia automatyzacji procesów. Dzięki temu podwoi się efektywność pracowników biurowych, a to oznacza uwolnienie ich czasu, który będą mogli



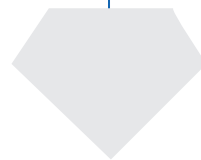
PRACOWNICY BĘDĄ MOGLI WYKORZYSTYWAĆ SWÓJ POTENCJAŁ TAM, GDZIE BĘDZIE ON NAJBARDZIEJ POTRZEBNY

spożytkować na realizację innych ważnych dla firm projektów. W praktyce oznacza to, że pracownicy będą mogli wykorzystywać swój potencjał tam, gdzie będzie on najbardziej potrzebny, znacząco zmniejszając swoje zaangażowanie w realizację monotonna i nudnych czynności, które można zautomatyzować. Może dotyczyć to m.in. przetwarzania danych – sortowania i kategoryzacji dokumentów oraz automatycznego generowania raportów i analiz czy też odpowiadania na standardowe zapytania klientów.

Musimy się nauczyć AI

Jest jednak też i druga strona medalu. IDC zwraca uwagę na wiele wyzwań, jakie stoją przed firmami (i nie tylko) w związku z wdrożeniem sztucznej inteligencji. Do najważniejszych zaliczają te związane z integracją nowych technologii z tymi już istniejącymi, koszty wdrożenia AI oraz brak specjalistów.

Wyzwania dotyczące rozwoju AI będą jednymi z tematów IDC Summit 2024, dwudniowej konferencji organizowanej w dniach 17–19 kwietnia w Sopocie.



AI

AUTOR

Michał Koch

Rewolucja w kreacji wideo

Firma OpenAI, twórcy ChatGPT, przedstawiła światu Sorę, innowacyjny model AI zdolny do tworzenia realistycznych wideo na podstawie prostego opisu. To zapowiedź nowej ery generowania treści wizualnych. Granica między rzeczywistością a kreacją staje się coraz bardziej nieostra.



Sora umożliwia generowanie klipów wideo na podstawie prompta, czyli kilkudzaniowego opisu połączonego z poleceniami. Otwiera to przed twórcami treści możliwości dotąd nieosiągalne. Wyobraźmy sobie potencjał – od edukacji po rozrywkę, od marketingu po sztukę... Możliwości są niemal nieograniczone. OpenAI, już osiągając sukces z ChatGPT, dąży do podwojenia przychodów do 2025 roku właśnie dzięki takim innowacjom.

OpenAI nie jest jedynym graczem na tym polu. Firmy technologiczne i start-upy – wśród nich jest zarówno Meta oraz Google, jak i Stability AI – również eksplorują możliwości AI w generowaniu wideo, co świadczy o dynamicznej i konkurencyjnej naturze tej dziedziny. To, jak ta konkurencja kształtuje przyszłość kreacji wideo i jakie narzędzia zostaną opracowane, aby zarządzać i moderować treści, będzie miało kluczowe znaczenie dla kierunku, w którym rozwinie się technologia generatywnego AI.

Nie brak jednak wyzwań. Eksperci biją na alarm wobec zagrożenia deepfake'ów i dezinformacji, szczególnie w kontekście wyborów. Doświadczaliśmy tego nawet w Polsce, gdy jesienią 2023 roku Platforma Obywatelska użyła AI do wygenerowania głosu ówczesnego premiera Mateusza Morawieckiego nie oznaczając jednak tego materiału jako stworzonego przez sztuczną inteligencję. Pewne jest, że media społecznościowe, już zmagające się z zalewem fałszywych treści, będą musiały stawić czoła ogromnej fali dezinformacji. To stawia ludzkość przed pytaniem: jak możemy



SZAREJ STREFY, W KTÓREJ BĘDZIE POWSTAWAŁ KONTENT WIDEO ŁAMIĄCY WYPRACOWANE JUŻ NORMY, ZAPEWNE JEDNAK NIE ZABRAKNIE. WSZAK JESTEŚMY W SIECI, TAM CZĘSTO ZASADY NIE OBOWIĄZUJĄ

równoważyć potencjał twórczy z odpowiedzialnością za etykę treści?

OpenAI zapowiada, że metadane będą kluczowe do identyfikacji wideo generowanych przez AI. To kluczowy krok w kierunku zapewnienia transparentności i prawdy w coraz bardziej wirtualnej rzeczywistości. Innowacja technologiczna musi iść w parze z etycznymi rozważaniami. Szarej strefy, w której będzie powstawał контент wideo łamiący wypracowane już normy, zapewne jednak nie zabraknie. Wszak jesteśmy w sieci, tam często zasady nie obowiązują.

Sora i podobne generatory wideo to niewątpliwie fascynujący krok w rozwoju sztucznej inteligencji. Otwarto drzwi dla nowych sposobów kreacji i ekspresji. Jednakże przed nami nie tylko korzystanie z tych innowacji, ale także aktywne kształtowanie rozwiązań prawnych oraz etycznych, aby technologia służyła dobru wspólnemu, zachowując równocześnie szacunek dla prawdy i autentyczności. Nasze podejście do innowacji i odpowiedzialności zdefiniuje, jak te narzędzia będą kształtować świat.

**Sora i podobne generatory
wideo to niewątpliwie fascynujący
krok w rozwoju.**



AI

AUTOR

Marek Nowak

AI w złych rękach

Każde narzędzie w niewłaściwych rękach może być groźne. Cyberprzestępcy na szeroką skalę wykorzystują sztuczną inteligencję do swoich celów. Na szczęście wiemy, jak nie dać się zaskoczyć.

Tuż po premierze ChatGPT okazało się, że w ramach życzliwego researchu potrafi on błyskawicznie przeszukać internet, by znaleźć na przykład podatności konkretnych modeli routerów i innych urządzeń telekomunikacyjnych. Szybko też w codziennym użyciu pojawiły się nowe pojęcia.



Phishing, spear phishing, spoofing

ChatGPT został uruchomiony pod koniec 2022 roku. W tym samym czasie, czyli od czwartego kwartału 2022 roku, raptownie wzrosła liczba złośliwych wiadomości phishingowych. Raport SlashNext przytacza w tym zakresie konkretną liczbę i mówi o wzroście na poziomie 1265 proc. Cyberprzestępcy wykorzystują sztuczną inteligencję przede wszystkim do automatycznego generowania treści e-maili. Stworzone przez AI wiadomości są spersonalizowane, przekonujące i trudne do odróżnienia od prawdziwych.

Sztuczna inteligencja pomaga również przestępcom podszywać się pod prawdziwe adresy e-mail oraz analizować publicznie dostępne informacje po to, by tworzyć ataki ukierunkowane, naśladować styl pisania i wzorce komunikacji nadawcy wiadomości.

– Narzędzia takie jak ChatGPT czy Google Bard posiadają wiele zabezpieczeń, które nie pozwalają im na tworzenie treści do wykorzystania w trakcie cyberataku. Nie można im zatem wydać bezpośredniego polecenia przygotowania e-maila, który mógłby posłużyć do przeprowadzenia ataku Business Email Compromise – mówi Mateusz Ossowski, CEE Channel Manager w firmie Barracuda Networks, która jest producentem rozwiązań z obszaru bezpieczeństwa IT. – Te ograniczenia można obejść, prosząc na przykład o wygenerowanie treści wiadomości od dyrektora zarządzającego do dyrektora finansowego z prośbą o pilne przepracowanie transakcji.

Znając ograniczenia oficjalnych narzędzi opartych na generatywnej sztucznej inteligencji, cyberprzestępcy

stworzyli nową usługę WormGPT. To dostępny w Dark webie chatbot, który służy do pisania złośliwego oprogramowania do tworzenia cyberataków, w tym do pisania poprawnych gramatycznie i ortograficznie e-maili phishingowych.

Napisz malware

Narzędzia takie jak WormGPT i EvilGPT dają też cyberprzestępcom inne, nowe możliwości. Atakujący mogą używać ich do zautomatyzowania swoich działań, w tym wyszukiwania i wykorzystywania podatności, tworzenia złośliwego oprogramowania, które jest w stanie modyfikować swoje zachowanie lub kod w odpowiedzi na napotkane środki bezpieczeństwa. Dodatkowo oparte na AI botnety mają potencjał do przeprowadzenia znanych chyba wszystkim małym i średnim operatorom telekomunikacyjnym w Polsce wyniszczających ataków rozproszonej odmowy dostępu do usługi (czyli DDoS). Przypomnijmy, że jest to także element toczącej się cyberwojny.

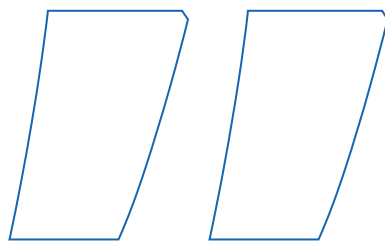
– Gdy ChatGPT zyskał na popularności, zauważyliśmy, że wiele osób prosi go o tworzenie skryptów automatyzacji za pomocą PowerShell lub podobnego narzędzia. Skrypty te często zawierały błędy, jednak nadal były pomocne i przyspieszały pracę administratorów. Tak samo ze sztucznej inteligencji korzystają dziś i w coraz większym stopniu korzystać będą cyberprzestępcy, tworząc złośliwe oprogramowanie. Jak wynika z wydanego niedawno raportu Barracuda Networks i Instytutu Ponemon, 48 proc. specjalistów IT uważa, że użycie generatywnej sztucznej inteligencji skróci czas potrzebny cyberprzestępcom do przygotowania cyberataku – komentuje Mateusz Ossowski.

Deepfake

Generowaniu fałszywych treści wizualnych i dźwiękowych przez sztuczną inteligencję poświęciliśmy niedawno odrębny artykuł. AI może też pomóc przestępcom w klonowaniu



**GDY CHATGPT
ZYSKAŁ NA
POPULARNOŚCI,
ZAUWAŻYLIŚMY, ŻE
WIELE OSÓB PROSI
GO O TWORZENIE
SKRYPTÓW
AUTOMATYZACJI
ZA POMOCĄ
POWERSHELL
LUB PODOBNEGO
NARZĘDZIA.
SKRYPTY TE CZĘSTO
ZAWIERAŁY BŁĘDY,
JEDNAK NADAL
BYŁY POMOCNE
I PRZYSPIESZAŁY
PRACĘ**



PODSZYWAJĄ SIĘ POD OSOBY ZARZĄDZAJĄCE, WYKORZYSTUJĄC ICH ADRESY E-MAIL, ZDJĘCIA A CZASEM TEŻ SPREPAROWANE NAGRANIA AUDIO, BY WYDAWAĆ POLECENIA AUTORYZACJI PRZELEWÓW

Nie jest tajemnicą, że wiele ataków e-mailowych tworzonych jest w innych krajach.

głosu, a co za tym idzie w podszywaniu się pod kogoś.

– Atakujący mogą przygotować deepfake’owe nagranie audio lub wideo, w którym wykorzystują głos czy wizerunek pracownika lub osoby z kadry kierowniczej firmy. Taki materiał dołączają do e-maila phishingowego, podnosząc jego wiarygodność. Cyberprzestępcy są w stanie także stworzyć fałszywe wideo, aby rozpowszechnić nieprawdziwe informacje o organizacji lub jej kierownictwie. Wszystko po to, by zaszkodzić reputacji i manipulować opinią publiczną – mówi Mateusz Ossowski z Barracuda Networks.

Inną taktyką wykorzystywaną przez cyberprzestępców jest przygotowywanie fałszywych spotkań wideo. Atakujący tworzą deepfake’owe filmy symulujące spotkania online lub konferencje z udziałem kierownictwa firmy. Podszywają się pod osoby zarządzające, wykorzystując ich adresy e-mail, zdjęcia a czasem też spreparowane nagrania audio, by wydawać polecenia autoryzacji przelewów lub udostępniania ekranów i przekazywania wrażliwych informacji.

Cyberprzestępcy uciekają się też do szantażów. Dzięki sztucznej inteligencji tworzą deepfake’owe filmy, w których ich ofiary biorą udział w kompromitujących lub niestosownych działaniach. Następnie atakujący próbują wymusić zapłatę okupu w zamian za niepublikowanie takich treści.

Tłumaczenie i lokalizacja

Nie jest tajemnicą, że wiele ataków e-mailowych tworzonych jest w innych krajach, przez osoby, które nie znają języka swojej potencjalnej ofiary. Nadal wiele takich e-maili ma charakterystyczne błędy gramatyczne, które są pierwszym sygnałem ostrzegawczym dla odbiorcy. Dzięki pomocy

sztucznej inteligencji przestępcy coraz łatwiej dostosowują jednak wiadomości phishingowe do lingwistycznego i kulturowego kontekstu odbiorców. Automatycznie tłumaczą wiadomości, odnoszą się do lokalnych wydarzeń kulturalnych, świąt, wiadomości lub zwyczajów, tworzą e-maile pisane branżowym językiem, z uwzględnieniem żargonu zrozumiałego dla atakowanej grupy osób, odnoszą się do lokalnych marek, instytucji lub organów rządowych.

Kradzież danych dostępowych

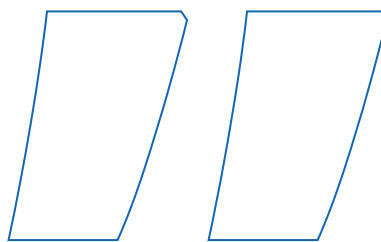
Kolejne działania cyberprzestępców, w których wykorzystywana jest sztuczna inteligencja to kradzież dostępu i poświadczeń. Hakerzy łatwiej tworzą fałszywe strony logowania przypominające prawdziwe. Sztuczna inteligencja po prostu ułatwia tworzenie kopii witryn. Szczególnie ważne staje się w związku z tym sprawdzenie (po adresie w oknie przeglądarki), czy rzeczywiście jesteśmy na stronie, na którą chcieliśmy trafić.

Hakerzy korzystają też z automatycznych, zasilanych przez AI narzędzi, aby systematycznie testować duże ilości kombinacji nazw użytkowników i haseł uzyskanych z poprzednich wycieków danych. Algorytmy sztucznej inteligencji optymalizują proces uzupełniania danych logowania, wybierając najbardziej prawdopodobne kombinacje na podstawie obserwowanych wzorców w przeciekach danych.

Narzędzia oparte na AI mogą też łamać hasła na podstawie dźwięku naciśnięć klawiszy. Zainfekowane złośliwym oprogramowaniem urządzenie umożliwia atakującemu podsłuchiwanie pomieszczenia i przechwytywanie wpisywanych haseł.

AI vs CAPTCHA

Ekspertami też przekonani, że skuteczna przestała być weryfikacja naszego ludzkiego postrzegania za pomocą CAPTCHA (Completely Automated



OSZUSTW Z PEWNOŚCIĄ BĘDZIE PRZYBYWAĆ, A UŻYTKOWNIKOM INTERNETU CORAZ TRUDNIEJ BĘDZIE SIĘ ZORIENTOWAĆ

Public Turing test to tell Computers and Humans Apart). Chodzi tu o testy polegające na odczytaniu zdeformowanego tekstu lub wykonaniu zadania typu: rozpoznaj i zaznacz wszystkie obrazki zawierające dany element.

AI w pokonaniu tego zabezpieczenia wspierają specjalne farmy CAPTCHA oraz skrypty działające na zasadzie rozpoznawania optycznego znaków (OCR). Dochodzi też do paradoksalnych sytuacji, gdy CAPTCHA skuteczniej zatrzymuje ludzi niż boty.

Oszustw z pewnością będzie przybywać, a użytkownikom internetu coraz trudniej będzie się zorientować, że padają ich ofiarami. Podstawą wydaje się dziś dwuetapowa weryfikacja podczas logowania, ostrożność przy otwieraniu wszelkich wiadomości (i linków) od znajomych, zwłaszcza tych, w których proszą o pieniądze. W razie wątpliwości dobrze jest po prostu zadzwonić lub dopytać, o co chodzi.

Niepokojące jednak pozostaje to, że nawet jeśli wydaje nam się, że rozmawiamy z daną osobą (i słyszymy jej głos), to nadal może być fake.



ENERGIA

AUTOR

**Klaudia
Wojciechowska**

Jak sztuczna inteligencja wpłynie na energetykę?

Dla sztucznej inteligencji i rozwoju produktów na niej opartych, rok 2023 był przełomowy. 2024 rok to zapewne dalszy rozwój AI, ale też wyzwania, jakie się z tym wiążą. Co stanie się z energetyką w tej sytuacji?

Rok 2023 to rok sztucznej inteligencji. Wzrosło zainteresowanie AI odbiorców prywatnych i firm. Największe budżety bigtechów i gospodarek uwzględniają ten aspekt. Wszyscy przewidują, że trend szybkiego rozwoju sztucznej inteligencji utrzyma się także w 2024 r.

Sztuczna inteligencja w UE

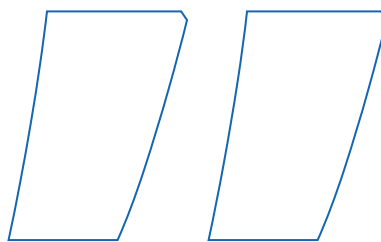
Unia Europejska w ramach programów *Horizon Europa* i *Cyfrowa Europa* planuje inwestować w AI. Na razie ma to być 1 mln euro rocznie. Ale już teraz Komisja Europejska szacuje,

że z czasem, mobilizując sektor prywatny i państwa członkowskie, będzie możliwe przeznaczanie na ten cel nawet 20 mld euro rocznie.

W tym samym czasie polityka unijna zacieśnia regulacje związane z efektywnością energetyczną. Wynika to z programu *Fit for 55*. Zakłada on ograniczenie emisji gazów cieplarnianych. To sygnał dla biznesu, że pora na bardziej *zielone* rozwiązania energetyczne dla, chociażby przetwarzania danych, które jest bardzo energochłonne.

Warto mieć to na uwadze także przy raportowaniu niefinansowym. To obowiązek coraz większej liczby firm. Przy współpracy z profesjonalnym dostawcą usług





centrodanowych czy chmury obliczeniowej, istotna będzie także efektywność energetyczna dostawcy.

W przypadku centrów danych istotny jest wskaźnik PUE. Określa on stosunek całości zużytej przez obiekt energii do ilości energii wykorzystywanej na potrzeby chłodzenia sprzętu IT. Średnia wartość PUE w Polsce wynosi 1,4–1,6. Obiekty, które mają wartość poniżej tej średniej, będą coraz bardziej cenione.

Istotny jest także rodzaj energii kupowanej przez dostawcę. Wykorzystanie źródeł odnawialnych do utrzymania infrastruktury IT znacząco redukuje carbon footprint (śląd węglowy). Do tego dochodzi także wskaźnik WUE – efektywność zużycia wody oraz polityka recyklingu sprzętu w data center. Czy w tym wszystkim przydatne będą rozwiązania oparte na AI? Czy może rozwój sztucznej inteligencji obciąży jeszcze bardziej systemy i zwiększy zużycie energetyczne?

2024 rok to rozwój centrów danych

Wpływ na sektor data center w 2024 r. będzie miała branża związana ze sztuczną inteligencją. To zmiany w obszarze projektowania obiektów centrów danych i konsumpcji energii. Związane jest to z tym, że utrzymanie infrastruktury IT pod

DLA DOSTOSOWANIA SIĘ DO NOWEJ TECHNOLOGII CENTRA DANYCH BĘDĄ MUSIAŁY ADAPTOWAĆ NOWE ROZWIĄZANIA CHŁODNICZE ORAZ ZMIENIĆ DESIGN WYPOSAŻANIA KOMÓR

Większość aktualnie dostępnych komórek serwerowych nie może być wykorzystywana do obsługi AI.



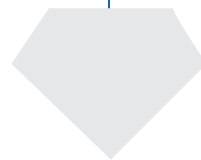
WSKAŹNIK PUE STAJE SIĘ ELEMENTEM KRYTYCZNYM. DLA BRANŻY AI OZNACZA TO KONIECZNOŚĆ WYBIERANIA DOSTAWCÓW O JAK NAJNIŻSZYCH WSKAŹNIKACH PUE

rozwiązania AI wymaga zupełnie innego podejścia. Tradycyjne rozwiązania konsumują między 4 a 25 kW/h na szafę rack. Zapotrzebowanie rozwiązań z obszaru sztucznej inteligencji jest na poziomie 60+ kW/h.

Oznacza to, że większość aktualnie dostępnych komór serwerowych nie może być wykorzystywana do obsługi AI. Dla dostosowania się do nowej technologii centra danych będą musiały adaptować nowe rozwiązania chłodnicze oraz zmienić design wyposażenia komór.

Wzrost atrakcyjności rozwiązań sztucznej inteligencji i większe nimi zainteresowanie to większe zapotrzebowanie na energię. Sprawia to, że wskaźnik PUE staje się elementem krytycznym. Dla branży AI oznacza to konieczność wybierania dostawców o jak najniższych wskaźnikach PUE. Dostawcy natomiast muszą liczyć się z koniecznością dalszego modernizowania komór wyposażonych w energooszczędne technologie chłodzące zasilane ze źródeł odnawialnych.





Z ŻYCIA MIŚOT

AUTOR

**Michał Koch,
Marek Nowak,
Klaudia
Wojciechowska**

Zjazd MiŚOT w Janowie Podlaskim – relacja

Zjazd MiŚOT w Janowie Podlaskim już za nami. Wydarzenie odbyło się pod hasłem Klaster Dzikiego Wschodu. Organizatorzy wyjaśnili, że to miejsce styku tego, co łączy każdego niezależnego małego i średniego operatora telekomunikacyjnego. Wiele działań biznesowych lepiej jest robić razem. O wielu rzeczach decydować jest łatwiej wspólnie.

W trakcie Zjazdu odbyło się 40 prelekcji i wykładów, prowadzonych równocześnie w trzech salach wykładowych, które stanowiły serce imprezy. W sumie ponad 300 uczestników wzięło udział, wśród nich było wiele nowych twarzy. Poruszono istotne tematy dotyczące funkcjonowania operatorów oraz wyzwiań, z jakimi się zmagają.

Zjazd Małych i Średnich Operatorów Telekomunikacyjnych w Janowie Podlaskim był

okazją do zdobywania wiedzy w dziedzinach prawa, marketingu oraz cyberbezpieczeństwa. Nie zabrakło także dyskusji w formule Hyde Park, która umożliwia bezpośrednią wymianę poglądów i doświadczeń między uczestnikami.

MdS pomoże wdrożyć NIS 2

Temat cyberbezpieczeństwa i wdrożenia dyrektywy NIS 2 spotkał się z dużym zainteresowaniem uczestników Zjazdu MiŚOT w Janowie Podlaskim.

Zgodnie z niedawnymi zapowiedziami wicepremiera i ministra cyfryzacji, Krzysztofa Gawkowskiego, nowy





projekt ustawy o krajowym systemie cyberbezpieczeństwa zostanie upubliczniony jeszcze w kwietniu. Będziemy mogli wówczas zobaczyć także całość zmian związanych z implementacją dyrektywy NIS2. Ustawa dotyczyć będzie też całego systemu odpowiedzialności za infrastrukturę krytyczną.

Marcin Zemła, ekspert z Projektu MdS, który wdraża już wymagania dyrektywy NIS 2 u operatorów z Grupy MiŚOT, podkreślił też, że pełnego wdrożenia przepisów nie da się dokończyć w kilka dni ani tygodni.

– Chcemy, abyście nadal mogli skupiać się na działalności telekomunikacyjnej w tych naprawdę trudnych warunkach, z którymi NATO oraz UE radzą sobie dziś, jak potrafią – mówi Marcin Zemła. – Chodzi zaś w tym wszystkim o to, aby trudniej było zdestabilizować Europę – podkreśla.

O realizacji projektów KPO i FERC

Temat realizacji projektów w konkursach KPO i FERC często przewija się we wszystkich dyskusjach małych i średnich operatorów telekomunikacyjnych. Nie mogło go również zabraknąć w trakcie Zjazdu MiŚOT w Janowie Podlaskim. Kwestie związane z realizacją projektów



W PIERWSZYM KONKURSIE SKŁADANIE PROJEKTÓW BYŁO BARDZIEJ DZIAŁANIEM HAZARDOWYM

przedstawiono od strony prawnej, a operatorzy, którzy realizują już konkretne projekty, mówili, co najbardziej utrudnia im prace i jakich zmian oczekivaliby w przyszłości.

– W pierwszym konkursie składanie projektów było bardziej działaniem hazardowym niż biznesowym – powiedział Sebastian Kachel, wiceprezes MiŚOT SA. – Nikt nie

NAD CZYM PRACUJEMY



- DALSZY WZROST WYDAJNOŚCI POPRZEZ OPTIMALIZACJĘ KODU
- MODEL DYSTRYBUCJI - TSEC W WERSJI PODSTAWOWEJ ORAZ DOSTĘP DO KANAŁÓW KONTAKTOWYCH Z NOC/SOC
- DOSTĘP DO PORTALU SZKOLENIOWEGO W CELU PODNIESIENIA WIEDZY SWOJEJ I SWOICH PRACOWNIKÓW.

SCRUBBING

WIŚNIEWSKI Z JAZZU MIŚOT



wiedział, jak to będzie. Teraz też często zgłaszając się do konkursu podejmujemy pewne ryzyko.

W dyskusji operatorzy zwracali też uwagę, że wiele procedur utrudnia im pracę, a może to być uproszczone, by całość przebiegała sprawniej. Problemy związane są [m.in.](#) z terminowością po stronie analizujących i rozliczających projekty. Czasem czeka się na odpowiedź bardzo długo i w tym czasie realizacja zadania jest zawieszona, co naturalnie przedłuża cały proces.

Pojawiła się też kwestia przesyłania przedsiębiorcom przez Centrum Projektów Polska Cyfrowa różnego rodzaju aneksów do posiadanych umów o dofinansowanie. To zmienia warunki biznesowe realizowanych już projektów i to w trakcie ich realizacji.

Uczestnicy dyskusji zwrócili też uwagę na terminowość i możliwość rozpoczęcia realizacji później niż dwa dni od podpisania umowy. Jeśli kilka projektów robi jeden operator, to powinien mieć możliwość rozłożenia ich w czasie.

Operator lokalny bliżej klientów

W drugim dniu Zjazdu MiŚOT w Janowie Podlaskim na Sali Głównej dużo czasu poświęcono działaniom marketingowym małych i średnich operatorów telekomunikacyjnych. Lokalni operatorzy powinni mieć świadomość, że choć mają mniejsze budżety na reklamę i ograniczone możliwości stosowania cen dumpingowych, to w wielu sytuacjach są na wygranej pozycji względem konkurencji. Bliskość klientów pozwala im lepiej dopasować ofertę i sposób komunikacji.

Łukasz Wiśniewski, ekspert od marketingu w sieci, opowiadał o schematach i mitach na jego temat, a także ostrzegał przed złymi praktykami, które mogą przynieść więcej szkody niż pożytku. Paweł Gniadek z MiŚOT SA

przedstawił niuanse związane z budową marki osobistej. Chociaż niektóre elementy wystąpienia pokrywały się z tym, co mówił poprzedni prelegent, tutaj nie skupiliśmy się wyłącznie na marketingu internetowym, ale mieliśmy okazję popatrzeć na zagadnienie szerzej.

Paneliści wspólnie zastanawiali się, jak uwzględnić w swojej ofercie potrzeby osób starszych, z niepełnosprawnościami czy z problemami finansowymi. W przypadku tych ostatnich operator lokalny ma lepsze możliwości podejścia do sprawy, gdyż działa na miejscu i często zna daną osobę od lat i wie, kiedy i z jakimi problemami się boryka.

– Operator lokalny inaczej podchodzi do klienta. W zależności od konkretnego problemu rozpatrujemy sprawę indywidualnie – powiedział Sebastian Pycia z Art.-Com.

Nie zabrakło też informacji o inicjatywie [Lokalni.pl](https://lokalni.pl), dzięki której operatorzy mogą w łatwy sposób dotrzeć do klientów. Opowiedziała o tym Aleksandra Czerach, liderka projektu:

– Udało nam się stworzyć dla operatorów działający produkt w ramach [Lokalni.pl](https://lokalni.pl). Oferujemy w jego ramach wszystko, co tworzy wizerunek nowoczesnej firmy.

Mali i średni operatorzy pomagają i nagradzają

Kapituła konkursu TeleOdpowiedzialny Roku 2023 dokonała wyboru dwóch laureatów nagrody głównej. Po dokładnej ocenie kilkudziesięciu aplikacji okazało się, że zarówno poznańska firma Systemia, jak i [Ostrog.net](https://ostrog.net) z Raciborza, uzyskały identyczną liczbę punktów. W związku z tym obie firmy zostały nagrodzone. Ponadto wręczono dziewięć dodatkowych wyróżnień.

– Gratulujemy zwycięzcom i wyróżnionym. Jesteśmy dumni, że z edycji na edycję aplikacje są ciekawsze i coraz mniej oczywiste.





Najoryginalniejsze nadal będziemy promować, aby również inni operatorzy mogli się nimi inspirować – mówiła podczas uroczystości Aleksandra Czerech, prezes Fundacji Lokalni.

– Mali i średni operatorzy telekomunikacyjni są coraz bardziej społecznie odpowiedzialni. Aktywnie wspierają potrzebujących, chronią środowisko, dbają o pracowników i otoczenie. Od sześciu lat to pokazujemy i najlepszych nagradzamy w naszym konkursie – powiedział Sebastian Kachel, wiceprezes Stowarzyszenia e-Południe, jeden z inicjatorów konkursu TeleOdpowiedzialny Roku.

Lokalni operatorzy, dążąc do efektywnego rozwoju swoich firm, pozostają niezależni i elastyczni. Kolejny Zjazd MIŚOT już jesienią!





TELEWIZJA

Cóż tam, panie, w telewizji?

AUTOR

Krzysztof Kołodziej

Od dawna nie działo się tak wiele w świecie telewizji. Od początku roku ruszyło osiem nowych kanałów, a Krajowa Rada Radiofonii i Telewizji ogłosiła konkurs na dwa kolejne. To oczywiście nie koniec. Oto przegląd wydarzeń na rynku telewizyjnym w pierwszym kwartale 2024.

Mogłoby się wydawać, że aktualna oferta prawie 300 polskich kanałów w zupełności zaspokaja apetyty operatorów. Do tego

stopnia, że wielu z programów nie mają nawet w swojej ofercie. Czołowi operatorzy żądają przy tym wysokich opłat za włączenie nowych kanałów. Dodatkowo płatny jest numer w EPG (elektroniczny przewodnik). Wysokość tych opłat dochodzi nawet do kilkudziesięciu tysięcy złotych miesięcznie. To jak widać nie zniechęca nadawców do tworzenia nowych projektów.

Prezentuję ich chronologiczny przegląd od początku roku.

Styczeń

10 stycznia na ogólnopolskim MUX-1 naziemnej telewizji cyfrowej pojawił się kanał Wydarzenia 24. Na MUX-4 stację zastąpił kanał Polsat News Polityka.

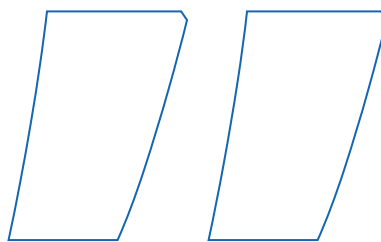
W październiku Krajowa Rada Radiofonii i Telewizji przyznała koncesję na MUX-1 kanałowi informacyjnemu W24. Nadawca zwrócił się do regulatora z wnioskiem o zmianę nazwy tej stacji na Wydarzenia 24. Jednocześnie poprosił o zmianę nazwy Wydarzeń 24 na Polsat News Polityka. KRRiT wyraziła na to zgodę.

Wydarzenia 24 można znaleźć na 49 pozycji telewizorów i dekoderów naziemnych, a Polsat News Polityka na 118 pozycji. Obie stacje są nadawane w standardzie DVB-T2/HEVC w jakości HD.

Luty

Pod koniec miesiąca Telewizja Media Narodowe poinformowała, że jest dostępna w Vectrze.





Operator nie miał jednak żadnej umowy z tym nadawcą. TVMN zaczęła bowiem nadawać na antenie lokalnej, radomskiej stacji ZebraTV. Po analizie sytuacji prawnej Vectra 1 marca usunęła ten kanał ze swojej oferty.

Marzec

Grupa MWE kończy przygotowania do uruchomienia czterech stacji.

2 z nich – [Pogoda24.TV](#) i Junior Channel ruszają 1 marca.

W serwisie Pilot WP rusza Benchmark TV. To szósta stacja Wirtualnej Polski, nadawana w modelu FAST.

Kanał Benchmark TV emituje treści poświęcone najnowszym gadżetom i trendom w świecie elektroniki.

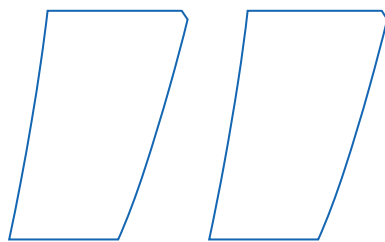
15 marca na MUX-8 pojawił się nowy kanał CTV9. Kanał jest dostępny na 50 pozycji dekoderek i telewizorów. Krajowa Rada Radiofonii i Telewizji zgodziła się na zmianę nazwy CTV9 na ViDoc TV. Reprezentująca kanał Red Carpet Media Group wzięła 2,5 miliona złotych pożyczki, aby częściowo opłacić koncesję kosztującą docelowo 17,85 miliona złotych.

Wyróżnikiem stacji ma być nowe spojrzenie na produkcje dokumentalne.

Kwiecień

2 kwietnia Wirtualna Polska uruchamia Kabalet TV, kanał telewizyjny w pełni poświęcony rozrywce. To pierwsza tego typu stacja

15 MARCA NA MUX-8 POJAWIŁ SIĘ NOWY KANAŁ CTV9. KANAŁ JEST DOSTĘPNY NA 50 POZYCJI DEKODERÓW I TELEWIZORÓW. KRAJOWA RADA RADIOFONII I TELEWIZJI ZGODZIŁA SIĘ NA ZMIANĘ NAZWY CTV9 NA VIDOC TV



RUSZYŁ RÓWNIEŻ KONKURS NA DWA KANAŁY NA MUX-8. PODMIOTY ZAINTERESOWANE NADAWANIEM NA ÓSMYM MULTIPLESIE, MAJĄ 45 DNI NA ZŁOŻENIE STOSOWNYCH WNIOSKÓW

w Polsce. Jej widzowie mogą oglądać kabarety przez 24 godziny na dobę.

Kabaret TV to druga, obok Telewizji WP, stacja należąca do Wirtualnej Polski Media.

3 kwietnia KRRiT zdecydowała o udzieleniu koncesji kanałowi Patronite Travel. To mieszanka autentycznych relacji podróżniczych, ekscytujących przygód oraz inspirowanych historii, które przybliżą różnorodność kultur, krajobrazów i ludzi na całym świecie.

Tego samego dnia ruszył również konkurs na dwa kanały na MUX-8. Podmioty zainteresowane nadawaniem

na ósmym multipleksie, mają 45 dni na złożenie stosownych wniosków. Przedmiotem konkursu jest rozpowszechnianie programu telewizyjnego o charakterze wyspecjalizowanym, tj. takiego, w którym nie mniej niż 70 proc. czasu nadawania w ciągu miesiąca, w godzinach 6.00–23.00, stanowić będą audycje i inne przekazy realizujące przyjętą specjalizację programu.

Wiadomo już, że w tym konkursie weźmie udział TV Republika, która ścigając się z TVN24 zamierza między innymi technicznie rozszerzyć swój zasięg.

8 kwietnia rozpoczęły nadawanie kanały Szlagier TV i TVC Super. Stacje trafiły na transponder platformy cyfrowej Canal+ na pozycji orbitalnej Hot Bird 13E i do MUX-L1, MUX-L3 oraz MUX-L4 naziemnej telewizji cyfrowej.

Szlagier TV można znaleźć na 67. pozycji dekodów Canal+, natomiast TVC Super na 60. Zastąpiły duble Power TV i Home TV na liście. Emisja jest niekodowana.

TVC Super promuje się hasłem Esencja Super Emocji. To kanał rozrywkowo-serialowo-filmowy.

Szlagier TV jest pierwszym 24 godzinnym kanałem ze szlagierami muzyki tradycyjnej i biesiadnej, oferując alternatywę dla disco polo i innych gatunków muzycznych.

To nie wszystkie nowości o których już wiemy, że się pojawią w tym roku. Warner Bros. Discovery z okazji i na czas Letnich Igrzysk Olimpijskich Paris 2024 uruchomi siedem dodatkowych kanałów HD i jeden kanał 4K.

Czeka nas szukanie dodatkowych programów poprzez dostrajanie odbiorników telewizyjnych, dekodów satelitarnych i aktualizacje boxów. Nasuwa się też pytanie: Skąd wziąć czas na oglądanie tych wszystkich nowości?

JAMBOX

TELEWIZJA ŚWIATŁOWODOWA

www.jambox.pl



DEKODERY IPTV
Arris 4302 **HD**
Arris 5202 **4K**



CatchUp
7 DNI WSTECZ



StartOver
OGLĄDAJ OD POCZĄTKU



JAMBO Nagrywarka
NAGRYWAJ W CHMURZE

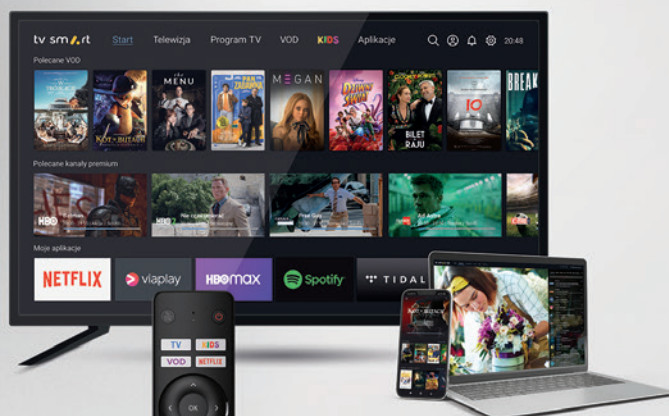


TELEFONIA KOMÓRKOWA

JAMBOX
mobile

LTE **5G**
VoLTE **Wi-Fi Calling**

tv smart



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.

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 dekodерów
- Zaawansowany system zarządzania usługami
- Dystrybucja usługi w multicast i unicast
- Wsparcie marketingowo-sprzedawcze

- **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



Podwyżka opłaty telekomunikacyjnej

Ministerstwo cyfryzacji planuje podnieść opłatę telekomunikacyjną. Protestuje przeciwko temu branża. Nie podoba jej się również brak rozwiązań ułatwiających dokonywanie zmian w umowach z abonentami.

Ministerstwo cyfryzacji przygotowuje projekt ustawy – Prawo komunikacji elektronicznej. Znalazła się w nim zmieniona stawka opłaty telekomunikacyjnej, którą każdego roku wnoszą przedsiębiorcy telekomunikacyjni. Stawka ma się zmienić z 0,05 proc. rocznych przychodów na 0,25 proc.

Uzasadnieniem podwyżki jest to, że stawka nie zmieniła się od 2004 r. Wpływy z niej są niższe niż wydatki Urzędu Komunikacji Elektronicznej i ministerstwa na zadania związane z telekomunikacją. W 2022 r. wyniosły 19,6 miliona PLN, co stanowiło 3,5-krotnie mniej niż wysokość wydatków.

Ministerstwo dodało, że istnieje próg zwolnienia z opłaty, który również ma zostać zmieniony. Obecnie zwolnienie dotyczy firm, których obroty w skali roku wynoszą do 4 mln PLN. Po zmianie progu będzie ustalany jako przeciętny przeciętny wynagrodzenia w gospodarce narodowej pomnożonego osiem tysięcy razy. W tym roku to 50,77 miliona PLN.

Zgodnie z przewidywaniami w 2024 r. przychody telekomów zobowiązanych do wnoszenia opłaty telekomunikacyjnej na nowych zasadach wyniosą około 36,1 miliarda PLN. Oznacza to 90,25 mln PLN z tytułu opłaty telekomunikacyjnej.

Operatorzy telekomunikacyjni przeciwni podwyżce

Branża telekomunikacyjna sprzeciwia się planowanej podwyżce opłaty telekomunikacyjnej. Polska Izba Informatyki i Telekomunikacji (PIIT) stwierdziła, że jest to działanie zdecydowanie niepożądane. Zgodnie z jej argumentacją nawet w obecnym kształcie wielkość wpływów jest waloryzowana. Przy stawce procentowej zależnej od rocznych przychodów podmiotu opłata rośnie wraz ze wzrostem tych przychodów.



Najlepszym sposobem podwyższania wpływów z jej tytułu jest stymulowanie rozwoju rynku telekomunikacyjnego, który w efekcie zwiększania swojej wartości wygeneruje wyższe dochody UKE – proponuje Polska Izba Informatyki i Telekomunikacji.

Przeciwko podwyżce jest nie tylko PIIT, ale również:

- ▶ Polska Izba Komunikacji Elektronicznej (PIKE),
- ▶ Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji (KIGEIT),
- ▶ Związek Pracodawców Mediów Elektronicznych i Telekomunikacyjnych Media-kom,
- ▶ Krajowa Izba Komunikacji Ethernetowej (KIKE),
- ▶ Fundacja Open Allies.

Propozycja znacznych podwyżek opłat administracyjnych związanych z telekomunikacją i zapowiedź ich regularnej waloryzacji jest o tyle niestosowna, że od lat działania administracji rządowej (w tym głównie UOKiK) w sposób niespotykany w innych krajach europejskich blokują przedsiębiorcom telekomunikacyjnym możliwość urealniania cen usług do rosnących kosztów – wyrażają swój sprzeciw izby.

Brak możliwości zmian w umowach

Innym problemem przedsiębiorców telekomunikacyjnych związanych z procedowanym Prawem komunikacji elektronicznej jest to, że nie zawiera ułatwień dotyczących możliwości dokonywania zmian w umowach z abonentami. Mogłyby one usprawnić urealnienie cen usług np. w przypadku inflacji. Chociaż Europejski kodeks łączności elektronicznej dopuszcza tego typu regulacje, to w Polsce są one właściwie niemożliwe.

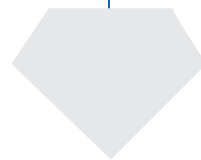
– Prawnie są one dopuszczalne, jednak interpretacje Urzędu Ochrony Konkurencji



TRUDNO STWIERDZIĆ, CZY PODWYŻKI ABONAMENTOWE WPROWADZANE Z UWAGI NA WYSOKĄ INFLACJĘ NIE SPOTKAJĄ SIĘ Z ZARZUTAMI. OSTATNIO PROBLEMY Z TEGO TYTUŁU MIAŁA VECTRA

i Konsumentów stawiają w tym zakresie wymogi, których nie da się spełnić. To czyni całe uprawnienie pozornym. Branża obawia się, że brak dodatkowych przepisów hamujących wymogi UOKiK spowoduje utrzymanie tej pozorności i stagnację branży, w której ceny nie nadążają za wzrostem kosztów – wyjaśnia Maciej Janowski, partner w Kancelarii Prawnej Media.

Z takiego niedoprecyzowania w przepisach wynikają problemy operatorów telekomunikacyjnych z klauzulami inflacyjnymi. Urząd Ochrony Konkurencji i Konsumentów bada kolejne sprawy i trudno stwierdzić, czy podwyżki abonamentowe wprowadzane z uwagi na wysoką inflację nie spotkają się z zarzutami z jego strony. Ostatnio problemy z tego tytułu miała Vectra.



Z PAMIĘTNIKA BEZPIECZNIKA

AUTOR

Marcin Zemła

NIS 2, czyli ja się chyba powieszę

Ja się chyba powieszę to pierwsza myśl, która przychodzi mi z każdym kolejnym, identycznym pytaniem dotyczącym unijnej dyrektywy NIS 2. Dlatego postanowiłem przed zjazdem w Janowie Podlaskim zrobić małą zbiorówkę dla środowiska, czyli dla tych, co chcą się czegoś dowiedzieć, dla tych, którym się wydaje, że coś wiedzą, dla tych, którzy jak zwykle wiedzą najlepiej oraz dla tych, dla których termin NIS 2, rewolucja w cyberbezpieczeństwie, SOC i podobne, to nowość i objawienie.



Na wstępie chciałem Wam zdradzić tajemnicę. Projekt MdS jest spółką Grupy MiŚOT dedykowaną dla security, działającą po to, abyście nie zostali z ręką w nocniku w momencie, gdy się w końcu obudzicie. Pomijam drobiazg, że budując swój telekomunikacyjny biznes, powinniście położyć bardzo silny nacisk na bezpieczeństwo. Pomijam też kolejny drobiazg zaciskających się aktów prawnych, które za chwile uniemożliwią Wam prowadzenie działalności, jeśli czegoś nie zrobicie, ale na litość, mamy wojnę! Mamy wojnę u nas w kraju! Nie kinetyczną jak na Ukrainie, ale jednak wojnę.

MdS jest dla Was

Projekt MdS ma spowodować, abyście nadal mogli skupiać się na działalności telekomunikacyjnej w tych naprawdę trudnych warunkach, z którymi NATO oraz UE radzą sobie dziś, jak potrafią. Czy im to dobrze idzie? To temat na inny artykuł. Chodzi w tym wszystkim o to, aby trudniej było zdestabilizować Europę – służba zdrowia w Irlandii, elektrownie (m.in. w Bełchatowie), ropa, gaz, protestujące ruchy społeczne a ostatnio rolnicy, to pokłosie tych prób.

Zajmujemy się przesyłaniem informacji i jest to istotny element obrony w dobie internetu. Czy chcecie tego, czy nie. Dlatego już od zgoła dwóch lat UE chce uszczelnić przestrzeń cyfrową, obdarzając ją nowymi wymogami zmierzającymi do większej kontroli. Dlatego Wasze protesty na zmieniającą się rzeczywistość mogą zostać, delikatnie mówiąc, *olane*. Łatwiej się bronić, mając do

dyspozycji kilka korporacji, które się szybko dostosowują, niż kilka tysięcy upartych operatorów, którzy opowiadają z dumą o *trzymielach w NASA*, na dowód własnego profesjonalizmu i nie zamierzają się doskonalić w dziedzinach istotnych dla obrony przestrzeni cyfrowej, bo mają na to... własny punkt widzenia. Sprawdza się on często do postawy: *póki nie karzą, to nic nie robimy*. Tyle gwoli wprowadzenia w sytuację.

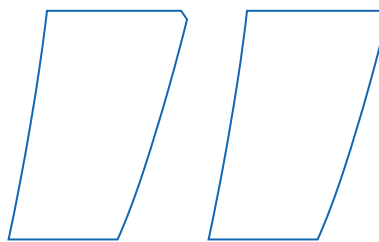
A teraz czas na opinie i pytania

NIS 2 **mnie dotyczy?!**

Wielu małych i średnich operatorów uważa, że dyrektywa NIS 2 ich nie dotyczy, bo prowadzą przedsiębiorstwa poniżej 50 osób zatrudnionych i 10 mln euro obrotu. To moja ulubiona opinia. Oczywiście błędna. Dyrektywa NIS 2 dotyczy Was wszystkich. Przepisy mówią jasno o *wszystkich dostawcach publicznych sieci łączności elektronicznej*. Artykuł 2 ust. 1 mówi zaś dokładnie: *Niniejsza dyrektywa ma zastosowanie do podmiotów publicznych lub prywatnych w rodzaju tych, o których mowa w załączniku I lub II, które kwalifikują się jako średnie przedsiębiorstwa na podstawie art. 2 załącznika do zalecenia 2003/361/WE lub które przekraczają pułapy dla średnich przedsiębiorstw określone w ust. 1 tego artykułu oraz które świadczą usługi lub prowadzą działalność w Unii*".

W artykule 2 ust. 2 czytamy: *Niniejsza dyrektywa ma również zastosowanie do podmiotów w rodzaju tych, o których mowa w załączniku I lub II, w przypadku gdy: a) usługi świadczone są przez: (i) dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej.*

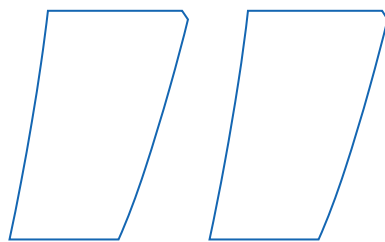
W artykule 3 dowiadujemy się natomiast: *Do celów niniejszej dyrektywy następujące podmioty uznaje się za podmioty kluczowe: dostawców publicznych sieci łączności elektronicznej*



WSZYSTKIE PODMIOTY, KTÓRE NIE ŁAPIĄ SIĘ NA DEFINICJĘ PODMIOTÓW KLUCZOWYCH ZGODNIE Z ART 3 UST. 1, ŁAPIĄ SIĘ NA DEFINICJĘ PODMIOTÓW WAŻNYCH

lub dostawców publicznie dostępnych usług łączności elektronicznej, które kwalifikują się jako średnie przedsiębiorstwa na podstawie art. 2 załącznika do zalecenia 2003/361/WE.

Oznacza to, że w większości MiŚOT-y nie będą podmiotami kluczowymi, jednak ten sam artykuł ustęp 2 wskazuje, że: *do celów niniejszej dyrektywy podmioty w rodzaju tych, o których mowa w załączniku I lub II, które nie kwalifikują się jako podmioty kluczowe zgodnie z ust. 1 niniejszego artykułu, uznaje się za podmioty ważne. Odnosi się to również do podmiotów, które zostały wskazane przez państwa członkowskie jako podmioty ważne zgodnie z art. 2 ust. 2 lit. b)–e).*



DLATEGO BŁAGAM, NIE BAWCIE SIĘ W ROSYJSKICH SZPIONÓW, ROZSIEWAJĄC DEZINFORMACJĘ NA ISPFORUM I W INNYCH MEDIACH, ŻE WAS TO NIE DOTYCZY, BO TO PO PROSTU NIEPRAWDA

Wszystkie podmioty, które nie łapią się na definicję podmiotów kluczowych zgodnie z art 3 ust. 1, łapią się na definicję podmiotów ważnych. Jak widzicie, występujecie w art. 2 ust. 2 lit a). To, że nie wskazano Was w art. 3 oznacza, że nie wyznacza Was państwo członkowskie, bo już to zrobiła Unia. Jak prześledzicie każdą z tych literek, poza (a), wymaga to jakiegoś wskazania. Was nie trzeba wskazywać, bo albo świadczycie te usługi, albo nie.

Różnicy w wymaganiach dla kluczowych i ważnych nie ma. Są jedynie w karach. Co do konkretów czekamy na polską ustawę. Nie może w niej jednak NIE BYĆ czegoś, co dyrektywa wymaga. Zarządzanie ryzykiem

w przedsiębiorstwie, badanie łańcucha dostaw, przeciwdziałanie zakłóceniom działalności, zaburzeniom integralności, dostępności, poufności oraz analizowanie i raportowanie incydentów sklasyfikowanych i korelujących z ryzykami – wszystko to będzie tam wpisane.

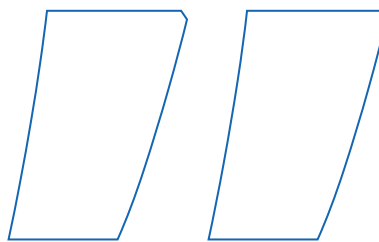
Dlatego błagam, nie bawcie się w rosyjskich szpionów, rozsiewając dezinformację na ISPFORUM i w innych mediach, że Was to nie dotyczy, bo to po prostu nieprawda.

Co to jest SOC?

SOC to Security Operation Center. Zespół ludzi świadczących kompleksowe usługi z zakresu bezpieczeństwa z użyciem różnych narzędzi. Wszystko zależy od branży.

Typowe usługi SOC to:

- ▶ monitoring podatności z alertami 24/7 (Blue Teaming);
- ▶ reakcje na alerty systemów klasy SIEM również przez 24h (Blue Teaming);
- ▶ reakcje na alerty systemów klasy NMS również przez 24h (Blue Teaming);
- ▶ ochrona antywirusowa, anti malware, anti ransomware również przez 24h (Blue Teaming);
- ▶ reakcje na zaburzenia zasad bezpieczeństwa (zagubienia, zniszczenia dokumentów, kradzież informacji, szpiegostwo, zaburzenia dostępności informacji w firmie, integralności informacji w firmie, poufności informacji w firmie) – tym zazwyczaj zajmuje się Pełnomocnik ds. Bezpieczeństwa;
- ▶ dbanie o nieprzerwane, niezakłócone działanie Systemu Zarządzania Bezpieczeństwem Informacji oraz Systemem Zarządzania Ciągłością Działania Firmy – tym również zajmuje się Pełnomocnik ds. Bezpieczeństwa;
- ▶ ochrona danych osobowych – tym zajmuje się Inspektor Ochrony Danych Osobowych;



- ▶ audyty bezpieczeństwa (Sprawdzenie bezpieczeństwa procesów w firmie w stosunku do jakiegoś szablonu. Są dwa: NIST (amerykański) i ISO 27001 – ten uwielbia UE. Nie da się go przejść, nie znając norm i zasad bezpiecznego zarządzania biznesem.) – Wewnętrzne Audyty prowadzi Pełnomocnik ds. Bezpieczeństwa a zewnętrzne Auditor Wiodący ISO27001;
- ▶ audyty systemów ciągłości działania (Wbrew nazwie nie chodzi o to, czy Wam routery i switche będą działały nieprzerwanie i jak to zabezpieczyliście. Tu chodzi o wprowadzenie procesów umożliwiających wyjście z zakłócenia głównie rynkowego działania Waszej firmy. Bardziej biznes niż technika.);
- ▶ testy penetracyjne (Zestaw działań zakontraktowanych zewnętrznie mający na celu obnażenie słabości Waszej działalności. Okresowo będziecie zmuszeni to zrobić. Nie chodzi tu tylko o Waszą infrastrukturę, ale również o zaburzenie dostępności, integralności i poufności informacji, które macie w firmie. Robi się to na zlecenie i zajmuje się tym Red Team.);
- ▶ testy wydajnościowe i stresujące (Są to testy aplikacji, usług i sieci komputerowych sprawdzające wytrzymałość rozwiązań, ich odporność na dużą skalę danych. Tu są ataki DDoS, testy wydajności routerów, serwerów, switche. Zajmują się tym na zlecenie Red Team w SOCu.);
- ▶ NOC -Network Operation Center (Zespół ludzi dbający o zmiany, konfiguracje i niezawodność usług w naszych węzłach. Również przez 24h.);
- ▶ szkolenia z nowych zagrożeń – tym zajmuje się Pełnomocnik ds. Bezpieczeństwa i IOD lub całe zespoły szkoleniowe.

Dlatego, gdy ktoś do Was przyjdzie i powie, że ma aplikacje lub pudełko, które daje Wam usługę SOC, pokażcie mu drzwi. Nie spełnicie w ten sposób wymagań ustawowych. Oczywiście możecie sami próbować to realizować.

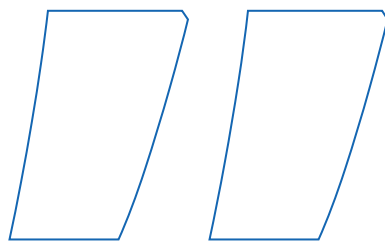
GDY KTOŚ DO WAS PRZYJDZIE I POWIE, ŻE MA APLIKACJE LUB PUDEŁKO, KTÓRE DAJE WAM USŁUGĘ SOC, POKAŹCIE MU DRZWI. NIE SPEŁNICIE W TEN SPOSÓB WYMAGAŃ USTAWOWYCH

Istnieje coś takiego jak SOC wewnętrzny. Są to ludzie pełniący te funkcje u Was w firmie. Tyle że kontrole sprawdzają kompetencje, skuteczność ochrony, a papiery są tutaj mniej ważne. Pamiętajcie, że są to osoby, które muszą zapewnić 24-godzinną ochronę zgodnie z polskim prawem, a to oznacza, że muszą pracować na zmiany. Inaczej zostanie to zakwestionowane.

Co to jest

System Zarządzania Bezpieczeństwem Informacji (SZBI)?

W dużym uogólnieniu to zbiór zasad wprowadzonych w firmie, który ma zapewnić bezpieczeństwo Twojego



ZARZĄDZANIE RYZYKIEM POWINNO OBEJMOWAĆ WSZYSTKIE ZAGROŻENIA DOTYCZĄCE TEGO, CO POSIADASZ W ZAKRESIE LUDZI, SPRZĘTU, DOKUMENTÓW, SYSTEMÓW I KONTAKTÓW

biznesu w zakresie dostępności informacji i usług, integralności (prawdziwości, niezaprzeczalności) oraz poufności, w każdym procesie, od dostawy usług lub komponentów, przez przetwarzanie tych informacji przez pracowników lub podwykonawców, skończywszy na świadczeniu tych usług klientowi i obsłudze reklamacji.

Normy opierają to na zarządzaniu ryzykiem. Tu ostrzeżenie. To, że ryzyka nie rozpoznałeś, nie oznacza, że jesteś bezpieczny w rozumieniu przepisów. Możesz się narażać na zarzut nierzetelności. Zarządzanie ryzykiem powinno obejmować wszystkie zagrożenia dotyczące tego, co posiadasz w zakresie ludzi, sprzętu, dokumentów, systemów i kontaktów.

Skąd mogę wziąć wzór polityki bezpieczeństwa?

Skąd chcesz. Firm sprzedających je (i to nawet dosyć tanio) jest na pęczki. Jest to jednak najgłębszy (i najprostszy) sposób zdobycia kar i zaliczania wpadek.

Polityka bezpieczeństwa jest dokumentem opisującym wymyślony przez Ciebie SZBI dla potrzeb Twojej firmy. Ta firma jest w jakimś środowisku, ma jakąś strukturę i jakieś zagrożenia. Inne zagrożenia ma każda firma. Dlatego najlepiej, abyś zrobił to sam dla swojej firmy albo z użyciem ludzi, którzy zrobią to za Ciebie.

Kupowanie *gotowców* nie da zgodności z przepisami. Firmy, które sprzedają takie kwity, według mnie, często po prostu naciągają klientów. Kupujesz swoje poczucie bezpieczeństwa, a to nie jest spełnieniem wymogów dyrektywy. Jedynym szablonem (przepisem) do zbudowania takiej polityki jest w UE norma ISO27001. Możesz ją sobie kupić. Normy są licencjonowane, więc nikt Ci ich nie da.

Jak zarządza się incydentami?

Po pierwsze trzeba je sklasyfikować. Dla przedsiębiorców telekomunikacyjnych są one sklasyfikowane na trzech poziomach: normalnym, poważnym i krytycznym.

Po drugie trzeba zrobić analizę ryzyka i monitorować coś, co nazwiemy incydentami.

Po trzecie trzeba to zgłaszać. Dziś do CSIRT NASK. Po wejściu ustawy zapewne do CSIRT TELCO. Służyć ma do tego system S46.

Po czwarte należy wyciągać wnioski z incydentów na podstawie ryzyk, jakie ze sobą niosą, wymyślać i wdrażać działania korygujące, aby te incydenty nie występowały w przyszłości.

I tu niespodzianka. Rejestr ryzyk musi korelować z rejestrem incydentów, ponieważ każdy incydent pogłębia jakieś ryzyko lub ujawnia nowe. Jedno i drugie musi być badane pod względem skuteczności wprowadzanych zmian w reakcji na nie. Inaczej, jak przyjdzie kontrola i zobaczy rejestry incydentów i ryzyk, będzie chciała zobaczyć dowody na wdrożenie działań minimalizujących te ryzyka i korygujących incydenty. I nie chodzi tu o papier. Właśnie dlatego nie kupujemy gotowców.

Dużo też zależy od przyjętych poziomów. Z jednej strony ograniczeniem są akty prawne, z drugiej zdrowy rozsądek ludzi, którzy z bezpieczeństwem pracują.

Czy da się mapować ryzyka zaciągnięte z internetu?

Niektóre tak, niektóre nie. Twoja firma różni się tysiącem rzeczy od innych firm. Nawet tych postawionych sto metrów obok Ciebie. Nie ma uniwersalnych ryzyk. Scenariusze może i są takie same, ale reakcja na nie i ocena ich skutków już nie. To sprowadza się do przesłania około pół tysiąca scenariuszy przy małej firmie i dbanie o to, żeby się później rozwijały i liczyły.

Czy jesteś w stanie zrobić to sam?

Niektóre rzeczy tak, niektóre nie. Audyty sam nie ogarniesz. Testów sam nie zrobisz. Możesz analizować incydenty i liczyć ryzyka, jeśli tylko zdobędziesz odpowiednią wiedzę i masz na to czas. Nie bardzo widzę skuteczne działanie jednoosobowego SOC 24/7. Zresztą mamy taki moduł w tSec do samodzielnego liczenia ryzyk i BIA. Nazywa się tRisk. Uprzedzam jednak, że z liczeniem incydentów i ryzyk jest jak z sieczkarnią: *Jeśli gównu wrzucisz, gównu wyjdzie.*

Ile czasu dostosowuje się działalność do NIS2?

Do NIS2, czyli do ISO27001. Dla bardzo małych MiŚOT-ów to około dwu miesięcy. Dla średnich MiŚOT-ów od dwóch do sześciu, dla dużych



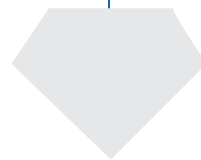
JAK ZROBISZ TO RZETELNIE, PIERWSZE EFEKTY PO WDROŻENIU ZOBACZYSZ PO ROKU

od sześciu do dwunastu. Dlaczego? Ponieważ rewolucja w zarządzaniu przedsiębiorstwem jest tym trudniejsza, im więcej jest w nim ludzi z określonymi przyzwyczajeniami, nierozpoznanych procesów, zależności, a także im większy jest obszar działalności i zróżnicowania klientów.

Jak zrobisz to rzetelnie, pierwsze efekty po wdrożeniu zobaczysz po roku. Tu już niezależnie od wielkości. Będziesz je widział w rachunku zysków i strat, najczęściej po stronie zmniejszonych strat (rok do roku).

Ile kosztuje dostosowanie do NIS2?

Jak jesteś mądry, to nic Cię to nie kosztuje. Mądry, czyli potrafisz policzyć pieniądze, które wydałeś i docenić brak strat, które ta inwestycja przyniosła. Dla ludzi liczących wprost: zapytajcie przedstawicieli Projektu MdS lub naszych przedstawicieli na Zjeździe MiŚOT. Hasła wywoławcze: *wdrożenie NIS2, usługa Pełnomocnika ds Bezpieczeństwa z IOD lub bez, SOC MdS.* Sprawdźcie też ceny rynkowe. Nie najdroższe, nie najtańsze. Schodzenie poniżej pewnych cen zwiększa ryzyko, że wydacie pieniądze, a i tak zaliczycie karę. Więc jak przy ubezpieczeniu raczej przenieście odpowiedzialność za fuckupy, a zwłaszcza kary administracyjne na takie właśnie firmy.



ZARZĄDZANIE

AUTOR

**Klaudia
Wojciechowska**

IP Scan w Polsce

MiŚOT-y mogą sprawdzić ochronę swoich własności intelektualnych

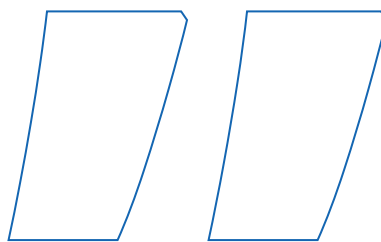
IP Scan jest usługą pozwalającą przedsiębiorcom na identyfikację poziomu ochrony własności intelektualnej w firmie. Wdrażanie jej w Polsce odbywa się we współpracy Urzędu Patentowego RP z Urzędem Unii Europejskiej ds. Własności Intelektualnej (EUIPO). Mikro, małe i średnie przedsiębiorstwa mogą otrzymać dofinansowanie na skorzystanie z tego rozwiązania.

Usługa IP Scan to część programu SME Fund (Fundusz dla MŚP). Zapewnia on dofinansowanie na zgłoszenia znaków towarowych, wzorów przemysłowych i wynalazków. Od kilku lat Polacy są w czołówce krajów UE, które ubiegają się o te środki z EUIPO. W 2023 r. zajęliśmy drugie miejsce, jeśli idzie o liczbę składanych wniosków. Było ich cztery tysiące.

Własność intelektualna to także wartość

Przedsiębiorca korzystający z usługi może wraz z ekspertem zweryfikować swoje zasoby związane z własnością intelektualną. Pozna też opcje wykorzystania ich dla zwiększenia zysków firmy. Raport z usługi IP Scan przygotowuje ekspert ds. własności intelektualnej. Będzie to osoba akredytowana przez Urząd Patentowy RP zgodnie z wymogami EUIPO.





Taki raport zawiera informacje i rekomendacje dotyczące:

- ▶ ochrony wynalazków,
- ▶ znaków towarowych,
- ▶ wzorów przemysłowych,
- ▶ tajemnicy przedsiębiorstwa,
- ▶ możliwości udzielania licencji do posiadanych przedmiotów własności przemysłowej.

Ma także uświadomić przedsiębiorcy ryzyko dotyczące naruszeń własności intelektualnej.

Jak skorzystać z IP Scan?

Mikro, małe i średnie przedsiębiorstwa mogą uzyskać 90 proc. dofinansowania na usługę IP Scan. To do 630 euro. Dotyczy to jednak wyłącznie sytuacji, w których wykonawca znajduje się na liście zamieszczonej na stronie Urzędu Patentowego RP.

W celu skorzystania z IP Scan należy złożyć wniosek, korzystając z aplikacji EUIPO. Po otrzymaniu pozytywnej decyzji Urzędu Unii Europejskiej ds. Własności Intelektualnej trzeba zgłosić chęć skorzystania z usługi do Urzędu Patentowego RP. Odbywa się to poprzez maila: ipscan@uprp.gov.pl. Po wybraniu wykonawcy z listy podpisuje się z nim umowę.

Tak przeprowadzona procedura pozwala przedsiębiorcy na uzyskanie dofinansowania działań. Jednak środki finansowane na to przeznaczone są ograniczone, dlatego decyduje kolejność zgłoszeń.

Więcej informacji można znaleźć na stronach Urzędu Patentowego Rzeczypospolitej oraz EUIPO.

**MIKRO, MAŁE
I ŚREDNIE
PRZEDSIĘBIORSTWA
MOGĄ UZYSKAĆ
90 PROC.
DOFINANSOWANIA
NA USŁUGĘ IP
SCAN. TO DO 630
EURO. DOTYCZY TO
JEDNAK WYŁĄCZNIE
SYTUACJI, W KTÓRYCH
WYKONAWCA
ZNAJDUJE
SIĘ NA LIŚCIE
ZAMIESZCZONEJ NA
STRONIE URZĘDU
PATENTOWEGO RP**



TRENDY

AUTOR

Michał Koch

Google wybierze za ciebie

Wszyscy zdajemy sobie sprawę, że największe korporacje używają ogromnych pieniędzy do zwiększania własnych wpływów na branżę technologiczną. Jednak czy wiedzieliście, że Google wydało w 2021 roku ponad 26 mld USD, aby być domyślną przeglądarką na różnych urządzeniach cyfrowych?

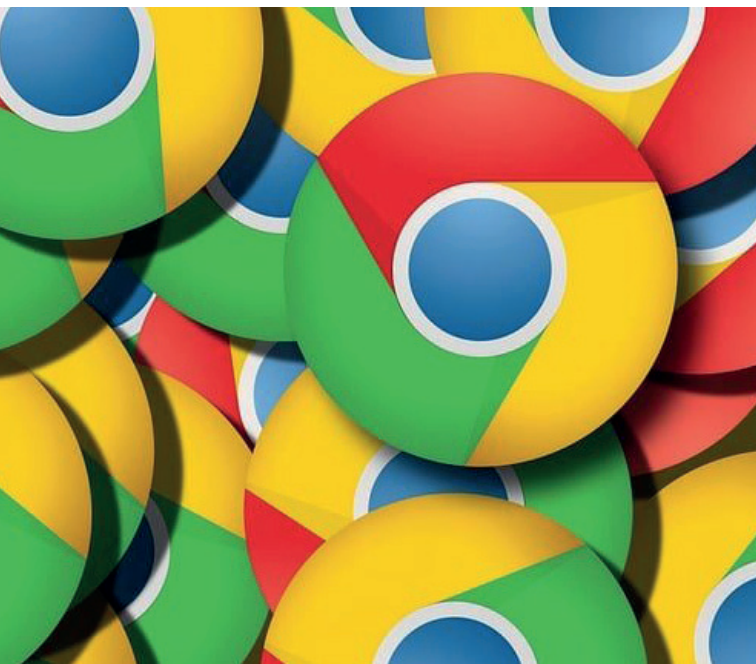
Zdobycie przez Google 90-proc. udziału na rynku przeglądarek internetowych – zarówno na urządzeniach stacjonarnych, jak i mobilnych – postronnym użytkownikom zapewne

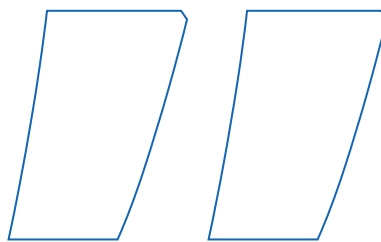
wydawało się czymś naturalnym. Po prostu: poszukujesz odpowiedzi na pytanie, więc używasz wujka Google'a.

Może jako konsumenci zostaliśmy po prostu wmianipulowani w korzystaniu z przeglądarki firmy z Kalifornii? Przecież jest jeszcze Opera, jest Firefox, jest i Safari. Okazuje się, że Google płaciło nawet Apple'owi, aby ich produkt był domyślnym web browserem. Do tej pory tajemnicą była przede wszystkim kwota takich świadczeń.

Sprawa wyszła na jaw przy okazji postępowania antymonopolowego, które prowadzi amerykański Departament Sprawiedliwości przeciwko Google'owi. Zeznania złożył Prabhakar Raghavan, starszy wiceprezes ds. wyszukiwania, reklam, handlu i płatności. Pracownik potwierdził, że firma od 2014 r. poczwórnice zwiększyła wydatki na ten cel (w 2014 r. wydano zaledwie 7,1 mld USD). Okazało się, że beneficjentami takich przelewów są m.in. wspomniane już Apple, ale też LG, Samsung i Motorola. Swoje otrzymują też operatorzy AT&T, T-Mobile oraz Verizon. Pieniądze mają wędrować nawet do twórców innych przeglądarek. Firma zarządzająca aktywami Bernstein szacuje, że w bieżącym roku Google może zapłacić Apple'owi aż 19 mld USD.

Na powyższy cel przeznaczono zatem astronomiczną kwotę. Jednak nic nie dzieje się bez przyczyny. W trakcie postępowania potwierdzono, że w ciągu minionych dziesięciu lat przychody Google'a wzrosły do 146 mld USD. Zatem wydatki się szybko (i pokaźnie) zwróciły.





ŚWIAT ZMIERZA KU KORPOKRACJI. WYSTARCZY ODPOWIEDNIO PRZYGOTOWAĆ PRZEKAZ, UŻYĆ TARGETOWANYCH REKLAM, OPŁACIĆ INFLUNCERÓW, DZIENNIKARZY I POLITYKÓW. NAJWIĘKSZE FIRMY MAJĄ ZASOBY, BY KSZTAŁTOWAĆ RZECZYWISTOŚĆ WZGLĘDEM WŁASNEGO WYOBRAŻENIA

Nikommu nie przeszkadzamy w zmianie domyślnej przeglądarki. Użytkownicy mogą to zrobić za pomocą kilku kliknięć – taki przekaz wychodzi z centrali Google'a. Spójrzmy jednak na to z innej strony. Czy aż 90 proc. internautów wybrałoby Google, gdyby rzeczywiście na rynku panowały równe zasady? Może ludzie – z natury leniwi – wolą, aby podsuwać im pewne rozwiązania pod nos? A może większość z nas nie ma nic przeciwko temu, że wybrano za nas?

Dlatego właśnie świat zmierza ku korporacji. Wystarczy odpowiednio przygotować przekaz, użyć targetowanych reklam, opłacić influencerów, dziennikarzy i polityków. Największe firmy mają zasoby, by kształtować rzeczywistość względem własnego wyobrażenia. Kiedy korporacje zaczną wybierać za nas coś więcej niż tylko internetowe przeglądarki? I czy wtedy w ogóle będziemy mogli jeszcze coś na to poradzić?

Zmienia się jednak sposób korzystania z internetu. Analitycy rynku wieszczą, że wkrótce to algorytmy sztucznej inteligencji, chociażby dobrze znany już ChatGPT, zastąpią obecnie znane nam przeglądarki. Zresztą pewna transycja dzieje się już teraz, na przykład Bing od Microsoftu – a od jakiegoś czasu też ChatGPT – mogą już korzystać z zasobów sieci, by podawać bardziej wiarygodne odpowiedzi. Google oczywiście nie chce przegapić tej zmiany, więc w 2017 r. uruchomiono spółkę Google AI, której zawdzięczamy model językowy BARD. Czyli zmieni się wszystko i nie zmieni się nic. The poor stay poor, the rich get rich.

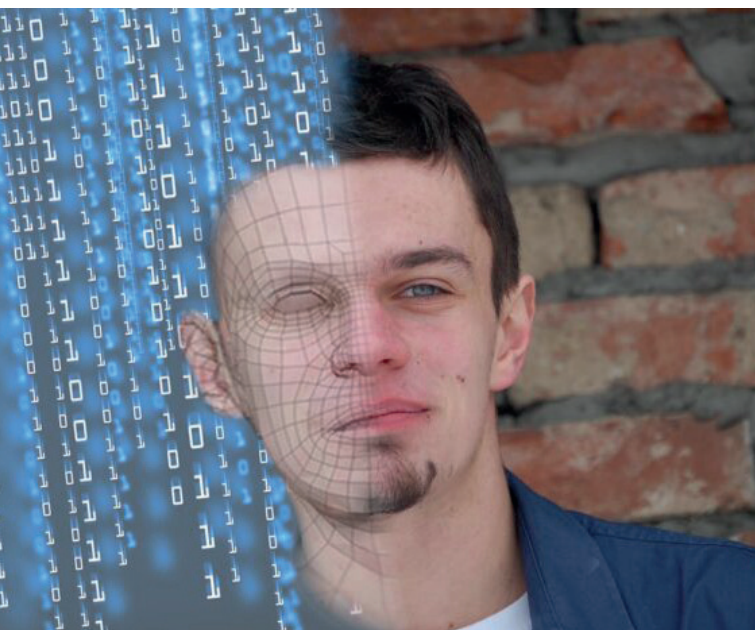


FELIETON

AUTOR
Michał Koch

Sztuczna inteligencja: od inspiracji do odpowiedzialności

Algorytmy AI stają się naszymi nieocenionymi pomocnikami. ChatGPT, generatywna sztuczna inteligencja stworzona przez OpenAI, zyskał popularność dzięki zdolności błyskawicznego generowania tekstów, tworzenia tłumaczeń, a nawet pomocy w tworzeniu całych procesów biznesowych. To wszechstronne narzędzie jest tym, o czym marzyło wielu pracowników i pracodawców. Sztuczna inteligencja nie jest jednak wolna od wyzwań, zwłaszcza tych związanych z RODO.



Przyjrzyjmy się następującej sytuacji: musimy napisać oficjalne pismo, a terminy gonią. ChatGPT może przyspieszyć ten proces, generując propozycje tekstu na podstawie naszych wytycznych. Jeśli potrzebujemy, to możemy poprosić nawet o kilka wersji. Tu czai się jednak pułapka. Trzeba pamiętać o RODO!

Wszystkie dane osobowe, które podajemy AI, są chronione. Na nas ciąży zatem obowiązek dbania o poprawne ich przechowywanie oraz przetwarzanie. Niezmiernie ważne jest to, że zanim prześlemy do ChatGPT naszego prompta (fragment tekstu, który służy jako polecenie dla systemu AI), zastanówmy się dwa razy, czy nie zawiera on danych poufnych.

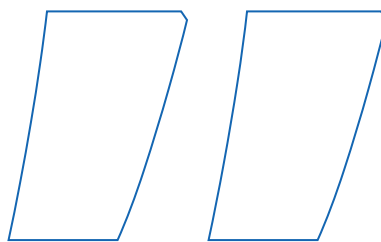
ChatGPT radzi sobie również z tłumaczeniami, umożliwiając szybką konwersję tekstu na różne języki. To nieocenione narzędzie w świecie, który jest globalną wioską, a bariery językowe mogą być poważną przeszkodą w komunikacji. Niemniej jednak jakość tłumaczenia może różnić się w zależności od języka i kontekstu, co wymaga od użytkowników ostrożności i ewentualnej weryfikacji. Zresztą weryfikację treści otrzymanej od AI zalecam za każdym razem. Przeprowadziłem już dziesiątki testów, a prawie zawsze znajduję coś do poprawy lub fakty, które nie do końca odpowiadają rzeczywistości. Szczególnie niechlujstwem był tekst, w którym ChatGPT beczelnie próbował wmówić mi, że jezioro Michigan znajduje się w Europie.

Co zatem z cyfryzacją dokumentów? Przecież tu nie powinno dochodzić do pomyłek, prawda? Przekształcając zeskanowane teksty do edytowalnych formatów, również mogą nam zdarzyć się przekłamania. Jednakże tu zalety przewyższają wady. Dzięki zdolnościom przetwarzania języka naturalnego AI może pomóc w transkrypcji audio na tekst, co jest szczególnie przydatne, gdy nagrania spotkań czy rozmów chcemy przerzucić do pliku tekstowego.

Jest jednak jeszcze jedna ważna kwestia, którą należy poruszyć. W miarę jak wdrażamy nowe technologie, takie jak sztuczna inteligencja, do naszego życia zawodowego i osobistego, musimy równie intensywnie inwestować w ochronę danych i infrastruktury, które je wspierają. Zaniedbanie tego aspektu może prowadzić do katastrofalnych skutków, od utraty ważnych danych, po szkody finansowe i reputacyjne. Bez tego cały ten postęp może okazać się sposobem na łatwy zarobek dla cyberprzestępców.

Bezpieczeństwo danych, zarówno naszych osobistych, jak i tych, które przetwarzają algorytmy AI, jest podstawą zaufania do nowych technologii. Inwestycje w zabezpieczenia, edukacja użytkowników oraz transparentne i zgodne z prawem zarządzanie danymi to filary, na których powinno opierać się wykorzystanie sztucznej inteligencji w codziennym życiu.

W cyfrowej epoce, w której dane są równie cenne jak złoto, ignorowanie zagrożeń związanych z cyberbezpieczeństwem jest jak żeglowanie na pełnym morzu bez kompasu. Odpowiednie zabezpieczenia nie tylko chronią nas przed cyberatakami, ale również budują zaufanie między technologią a jej użytkownikami. Przykład ChataGPT pokazuje, jak bardzo zaawansowane narzędzia mogą wspierać ludzi w pracy i życiu codziennym, jednak bez odpowiedniej troski o aspekty prawne i bezpieczeństwo, ryzykujemy utratę więcej niż tylko danych.



ZADBAJMY WIĘC O TO, BY POSTĘP TECHNOLOGICZNY SZEDŁ W PARZE Z ROZWIJANIEM ŚWIADOMOŚCI I SYSTEMÓW OCHRONY, KTÓRE ZAPEWNIĄ, ŻE KORZYSTANIE Z INNOWACJI BĘDZIE BEZPIECZNE I EFEKTYWNE

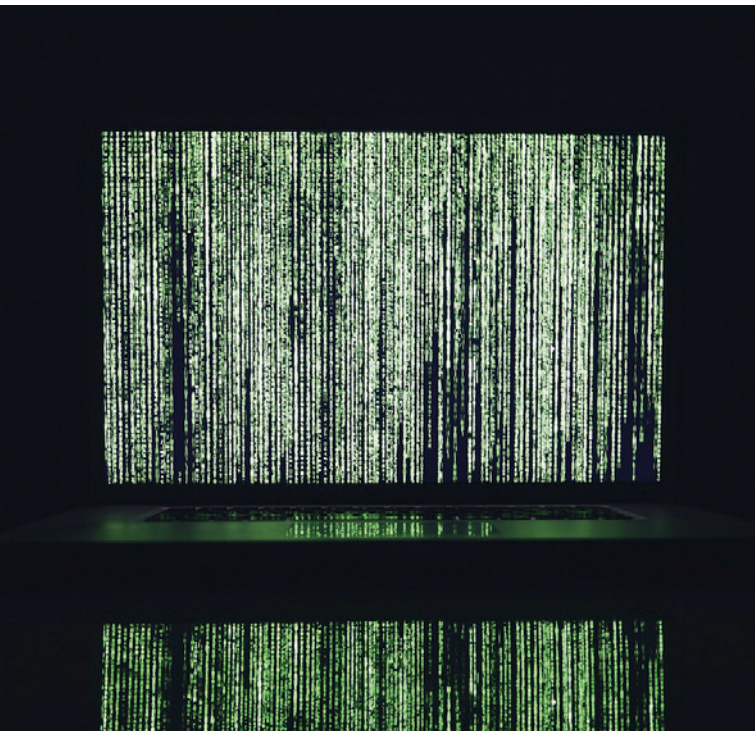
Pamiętajmy, że to nie tylko technologia, ale i odpowiedzialność za nią definiuje przyszłość. Zadbajmy więc o to, by postęp technologiczny szedł w parze z rozwijaniem świadomości i systemów ochrony, które zapewnią, że korzystanie z innowacji będzie bezpieczne i efektywne dla wszystkich.



Wirtualizacja Proxmox – typy magazynów danych

Wstęp

Model przechowywania danych w Proxmox VE jest bardzo elastyczny. Obrazy maszyn wirtualnych mogą być przechowywane na jednym lub kilku lokalnych nośnikach danych, lub na współdzielonym zasobie, takim jak NFS lub iSCSI (NAS, SAN). Można jednocześnie korzystać z wszystkich technologii przechowywania dostępnych w systemie Debian Linux.

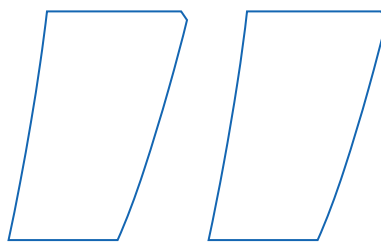


Do zarządzania magazynami danych, Proxmox używa biblioteki **libpve-storage-perl**. Wykorzystuje ona elastyczny system wtyczek, aby zapewnić wspólny interfejs dla wszystkich typów przechowywania. Dzięki czemu większość konfiguracji magazynów danych może zostać przeprowadzona z wykorzystaniem GUI.

Typy storage (magazyny danych) można podzielić na:

Zdalne (zasoby współdzielone)

1. Współdzielenie danych między węzłami: Przechowywanie danych jest dostępne dla wszystkich węzłów w klastrze Proxmox. Węzły mogą uzyskać dostęp do tych danych poprzez sieć.
2. Live migration i wysoka dostępność: Jedną z głównych zalet współdzielonego przechowywania jest możliwość migracji na żywo działających maszyn wirtualnych między węzłami bez przestoju usług, ponieważ wszystkie węzły mają dostęp do tych samych danych.
3. Elastyczność i skalowalność: Współdzielone przechowywanie pozwala na elastyczne zarządzanie zasobami i skalowanie infrastruktury, umożliwiając dodawanie nowych węzłów i zwiększanie pojemności przechowywania w miarę potrzeb.



Lokalne

1. Prostota konfiguracji: Lokalne przechowywanie jest łatwe do skonfigurowania, ponieważ polega na wykorzystaniu dysków twardych bezpośrednio podłączonych do serwera Proxmox.
2. Wysoka wydajność: Dostęp do danych odbywa się bezpośrednio z lokalnych dysków, co często zapewnia szybszy dostęp w porównaniu do przechowywania danych na zdalnych nośnikach.
3. Brak współdzielenia z innymi węzłami: Lokalne przechowywanie nie jest współdzielone między węzłami w klastrze Proxmox. Każdy węzeł ma dostęp tylko do swojego lokalnego przechowywania.

Plikowe

1. System plików na poziomie hosta: Przechowywanie plikowe polega na zapisywaniu maszyn wirtualnych jako plików na systemie plików hosta. Każda maszyna wirtualna jest przechowywana jako pojedynczy plik.
2. Elastyczność w zarządzaniu: Przechowywanie plikowe jest elastyczne i łatwe w zarządzaniu, ponieważ pozwala na łatwe kopiowanie, przenoszenie i tworzenie kopii zapasowych plików maszyn wirtualnych.
3. Prostsza konfiguracja: Konfiguracja przechowywania plikowego jest zazwyczaj prostsza niż przechowywanie blokowe, ponieważ nie wymaga konfiguracji specjalnych urządzeń blokowych.
4. Dostęp do plików przez sieć: W przypadku przechowywania plikowego pliki maszyn wirtualnych mogą być dostępne przez sieć, co umożliwia łatwe udostępnianie maszyn wirtualnych innym systemom.

Blokowe

1. Dysk jako urządzenie blokowe: Przechowywanie blokowe polega na korzystaniu z dysków twardych lub macierzy RAID jako

PRZECHOWYWANIE BLOKOWE POLEGA NA KORZYSTANIU Z DYSKÓW TWARDYCH LUB MACIERZY RAID JAKO URZĄDZEŃ BLOKOWYCH DO PRZECHOWYWANIA MASZYN WIRTUALNYCH

- urządzeń blokowych do przechowywania maszyn wirtualnych.
2. Wydajność: Przechowywanie blokowe może oferować lepszą wydajność niż przechowywanie plikowe, ponieważ dostęp do danych odbywa się bezpośrednio poprzez urządzenia blokowe.
3. Złożoność konfiguracji: Konfiguracja przechowywania blokowego może być bardziej złożona niż przechowywania plikowego, ponieważ wymaga to zarządzania dyskami twardymi, partycjami i/lub macierzami RAID.
4. Współdzielone przechowywanie: Przechowywanie blokowe może być łatwiej współdzielone między wieloma węzłami w klastrze, co umożliwia migrację maszyn wirtualnych na żywo i wysoką dostępność.

Przegląd obsługiwanych magazynów danych.

Description	Plugin type	Level	Shared	Snapshots	Stable
ZFS (local)	zfspool	both ¹	no	yes	yes
Directory	dir	file	no	no ²	yes
BTRFS	btrfs	file	no	yes	technology preview
NFS	nfs	file	yes	no ²	yes
CIFS	cifs	file	yes	no ²	yes
Proxmox Backup	pbs	both	yes	n/a	yes
GlusterFS	glusterfs	file	yes	no ²	yes
CephFS	cephfs	file	yes	yes	yes
LVM	lvm	block	no ³	no	yes
LVM-thin	lvmthin	block	no	yes	yes
iSCSI/kernel	iscsi	block	yes	no	yes
iSCSI/libiscsi	iscsidirect	block	yes	no	yes
Ceph/RBD	rbd	block	yes	yes	yes
ZFS over iSCSI	zfs	block	yes	yes	yes

Domyślna konfiguracja Proxmox

W większości przypadków nie ma konieczności konfiguracji **storage** z poziomu linii komend i większość zadań można przeprowadzić za pomocą GUI. Cała konfiguracja przechowywana jest w pliku `/etc/pve/storage.cfg`.

Domyślna instalacja Proxmox posiada następującą konfigurację:

dir: **local**

path /var/lib/vz
content iso,vztmpl,backup

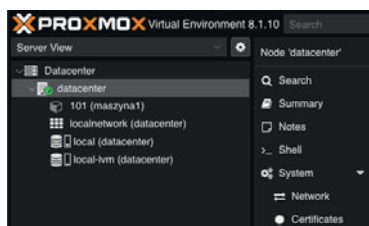
lvmthin: **local-lvm**

thinpool data
vgname pve
content rootdir,images

Widzimy tutaj dwa magazyny danych: **local** oraz **local-lvm**. Inną metodą weryfikacji jest użycie komendy:

```
root@datacenter:~# pvesm status
Name      Type      Status      Total      Used      Available      %
local     dir       active      26594276   5394324   19823696      20.28%
local-lvm lvmthin   active      20905984   639723    20266260      3.06%
```

Lub z poziomu GUI



Magazyn **local** jest to **storage** typu **katalog** (przechowuje dane jako pliki), który zawiera: obrazy ISO, szablony kontenerów, oraz backupy maszyn

Magazyn **local-lvm** jest to **storage** typu **lvmthin** (dane blokowe), który przechowuje dyski maszyn wirtualnych oraz kontenerów w postaci wolumenów logicznych.

LVM - Logical Volume Manager

Linux Logical Volume Manager (LVM) to narzędzie umożliwiające elastyczne zarządzanie przestrzenią dyskową na systemach Linux. Oto kilka kluczowych cech i funkcji Linux LVM:

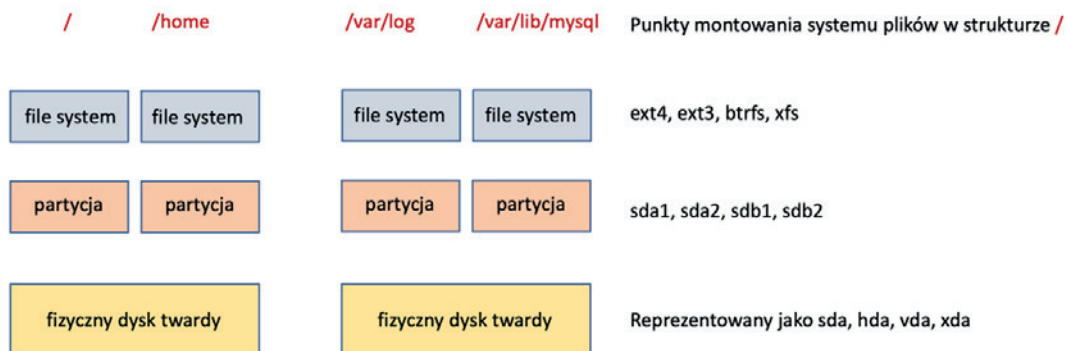
1. Logical Volumes (LV): LVM umożliwia tworzenie logicznych woluminów (LV), które są abstrakcyjnymi warstwami nad fizycznymi partycjami dyskowymi lub dyskami. Dzięki LV, można dynamicznie zarządzać przestrzenią dyskową, tworząc, usuwając, zmieniając rozmiar i łącząc woluminy w zależności od potrzeb.
2. Volume Groups (VG): Grupy woluminów (VG) są zbiorami dysków fizycznych lub partycji, które są łączone w jedną logiczną jednostkę zarządzania przestrzenią dyskową. LV są tworzone w obrębie VG
3. Physical Volumes (PV): Fizyczne woluminy (PV) są to dyski twarde lub partycje, które są dodawane do grup woluminów (VG) w celu tworzenia logicznych woluminów (LV). LVM obsługuje różne typy fizycznych woluminów, w tym dyski twarde, partycje, dyski sieciowe i urządzenia blokowe.

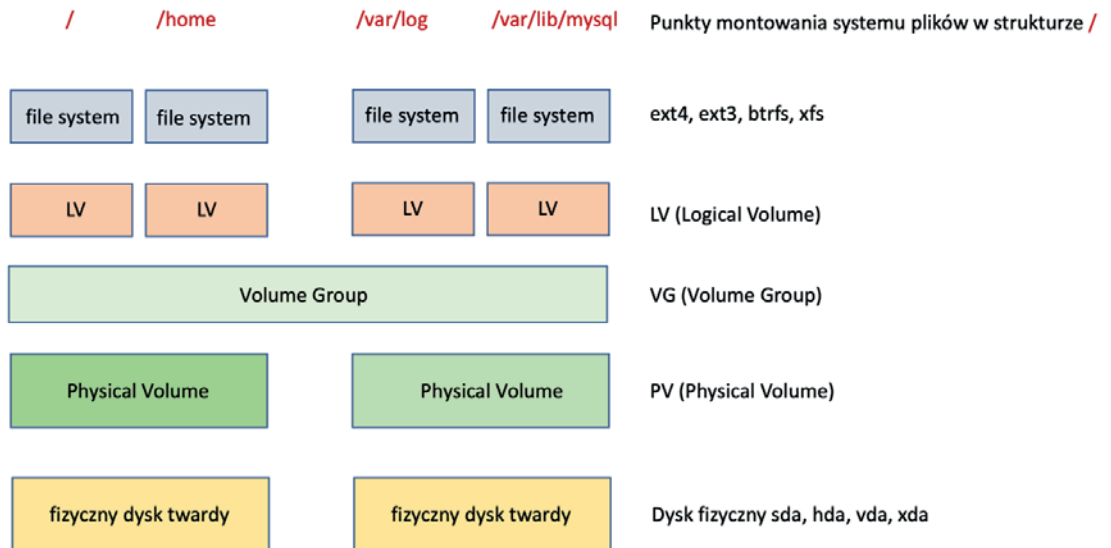
4. Dynamiczne skalowanie: Jedną z najważniejszych cech LVM jest możliwość dynamicznego skalowania LV i VG bez konieczności przerywania działania systemu. Można zwiększać rozmiar LV, VG oraz dodawać nowe dyski fizyczne bez konieczności przerywania pracy systemu.
5. Snapshoty: LVM umożliwia tworzenie migawek (snapshotów) logicznych woluminów, co pozwala na wykonywanie kopii zapasowych oraz wykonywanie eksperymentów na danych bez ryzyka utraty oryginalnych danych.

Mirroring i Striping: LVM obsługuje funkcje RAID, takie jak mirroring i striping, co umożliwia zwiększenie wydajności i niezawodności poprzez replikację danych na różnych dyskach fizycznych.

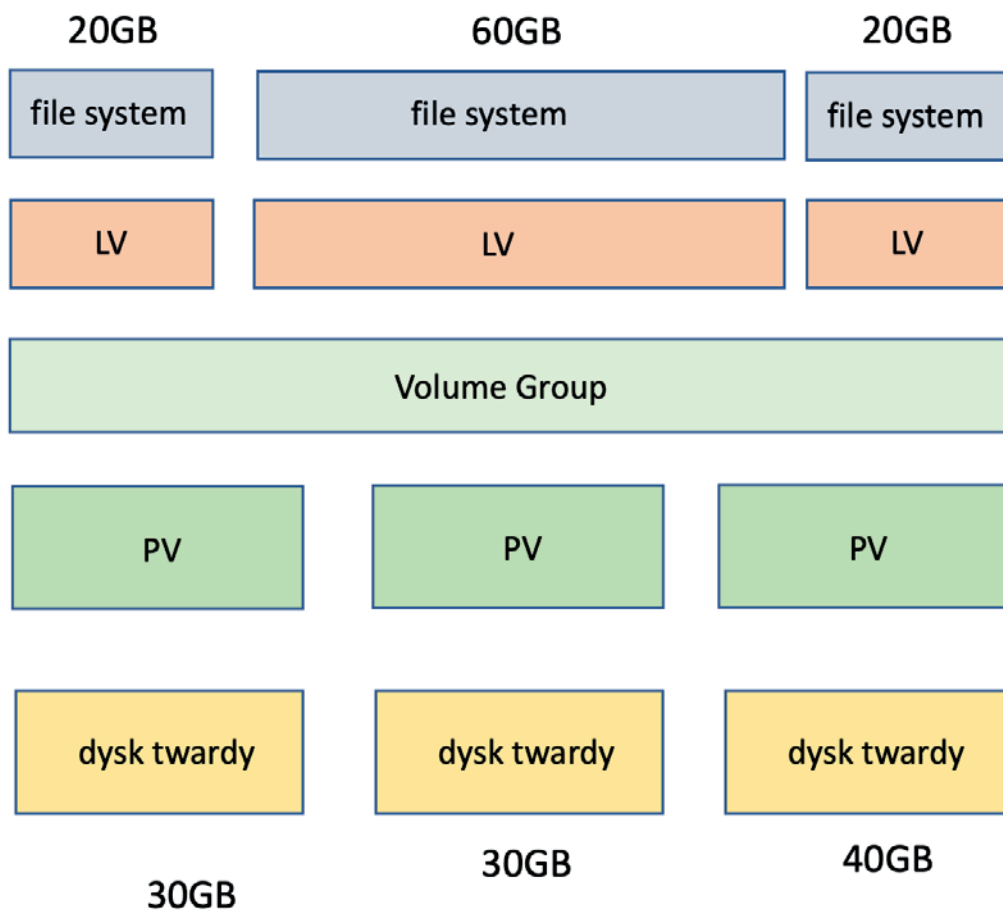
Aby przybliżyć architekturę LVM, posłużymy się analogią do klasycznego modelu partycjonowania dysków.

W przypadku konfiguracji LVM mamy następujący schemat:





Jak widzimy struktura LVM jest bardziej złożona od klasycznego schematu partycjonowania. Jednak zyskujemy cały szereg opisanych wcześniej funkcjonalności niedostępnych w klasycznym modelu partycjonowania. Jedną z podstawowych zalet LVM jest możliwość elastycznego zwiększania rozmiaru grupy wolumenów (Volume Group) i tworzenie wolumenów logicznych o rozmiarach większych niż rozmiar pojedynczego dysku fizycznego.



Aby praktycznie pokazać możliwości LVM, wykonamy zadanie polegające na zwiększeniu rozmiaru magazynu danych lvm-local poprzez dodanie nowego dysku o pojemności 60GB. Weryfikacja rozmiaru aktualnie posiadanego miejsca.



Widzimy 21GB. Następnie do serwera dodajemy dysk 60GB. Sprawdzamy, czy dysk jest widoczny w serwerze Proxmox.

The screenshot shows the Proxmox VE interface for the 'Node: datacenter' view, specifically the 'Disks' section. A table lists the disks, including a new 64.42 GB disk labeled /dev/sdb.

Device	Type	Usage	Size	GPT	Model	Serial	S.M.A.R.T.	M...	Wearout
/dev/sda	unknown	partitions	68.72 GB	Yes	QEMU_HARDDISK	drive-sda0	OK	No	N/A
/dev/sda1	partition	BIOS boot	1.03 MB	Yes				No	N/A
/dev/sda2	partition	EFI	536.87 MB	Yes				No	N/A
/dev/sda3	partition	LVM	68.16 GB	Yes				No	N/A
/dev/sdb	unknown	no	64.42 GB	No	QEMU_HARDDISK	drive-sdb1	OK	No	N/A

Jak widać pojawił się dysk oznaczony jako **/dev/sdb**. Należy go zainicjować za pomocą komendy **pvcreate**, a następnie zweryfikować komendą **pvdisplay**.

```
root@datacenter:~# pvcreate /dev/sdb
Physical volume "/dev/sdb" successfully created.
root@datacenter:~# pvdisplay
--- Physical volume ---
PV Name           /dev/sda3
VG Name           pve
PV Size           <63.50 GiB / not usable 2.98 MiB
Allocatable       yes
PE Size           4.00 MiB
Total PE          16255
Free PE           2017
Allocated PE      14238
PV UUID           qfNkwc-jCKn-uAQw-LKxh-6QaP-QEME-QTWLxr

"/dev/sdb" is a new physical volume of "60.00 GiB"
--- NEW Physical volume ---
PV Name           /dev/sdb
VG Name           pve
PV Size           60.00 GiB
Allocatable       NO
PE Size           0
Total PE          0
Free PE           0
Allocated PE      0
PV UUID           MSknw1-yuXY-6ESv-mVxS-cBKe-BYrV-wjYekZ
```


Kolejnym krokiem jest zwiększenie rozmiaru grupy wolumenów **pve** oraz **pve/data**.

```
root@datacenter:~# vgextend pve /dev/sdb
Volume group "pve" successfully extended

root@datacenter:~# lvextend -L+60G pve/data
Size of logical volume pve/data_tdata changed from <19.94 GiB (5104 extents) to <79.94 GiB (20464 extents).
Logical volume pve/data successfully resized.
root@datacenter:~# lvresize --poolmetadatasize +1GB pve/data
Size of logical volume pve/data_tmeta changed from 1.00 GiB (256 extents) to 2.00 GiB (512 extents)
Logical volume pve/data_tmeta successfully resized.
```

Na koniec weryfikacja z poziomu GUI.



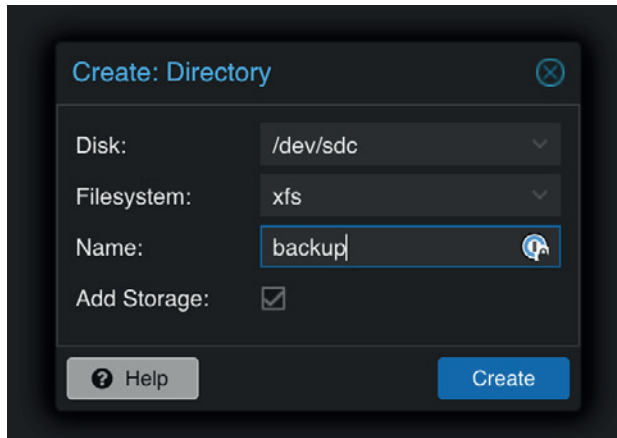
Powyższą procedurę należy powtórzyć dla każdego nowo dodanego dysku.

Katalog

Dowolny katalog w systemie plików Linux może zostać zainicjowany jako magazyn danych. W tym przykładzie posłużymy się nowo dodanym dyskiem. Procedura dodania dysku z linii komend zakłada ustawienie partycji, założenie systemu plików i podmontowanie go. W Proxmox możemy te wszystkie czynności wykonać z GUI.

Device	Type	Usage	Size	GPT	Model	Serial	S.M.A.R.T.	M...	Wearout
/dev/sda	unknown	partitions	68.72 GB	Yes	QEMU_HARDDISK	drive-scsi0	OK	No	N/A
/dev/sda1	partition	BIOS boot	1.03 MB	Yes				No	N/A
/dev/sda2	partition	EFI	536.87 MB	Yes				No	N/A
/dev/sda3	partition	LVM	68.18 GB	Yes				No	N/A
/dev/sdb	unknown	LVM	64.42 GB	No	QEMU_HARDDISK	drive-scsi1	OK	No	N/A
/dev/sdc	unknown	No	34.38 GB	Yes	QEMU_HARDDISK	drive-scsi2	OK	No	N/A

Klikamy **Initialize Disk with GPT**, następnie w sekcji **Directory** wybieramy **Create: Directory**.



W ten sposób został zainicjowany nowy dysk, utworzony nowy katalog, na którym możemy przechowywać:

- ▶ backupy maszyn
- ▶ dyski maszyn wirtualnych/kontenerów
- ▶ obrazy ISO
- ▶ szablony kontenerów

NFS – Network File System

Network File System (NFS) w Proxmox to protokół umożliwiający współdzielenie plików i dostęp do nich poprzez sieć. NFS jest często używany w środowiskach wirtualizacyjnych, takich jak Proxmox, do przechowywania obrazów maszyn wirtualnych oraz danych konfiguracyjnych. Oto kilka kluczowych cech NFS w Proxmox:

1. Współdzielenie danych: NFS umożliwia udostępnianie danych przechowywanych na zdalnych serwerach przez sieć. W przypadku Proxmox, serwery NFS mogą być używane do przechowywania obrazów dysków maszyn wirtualnych oraz plików konfiguracyjnych.
2. Montowanie zdalnych zasobów: Serwery Proxmox mogą montować zdalne zasoby NFS jako lokalne katalogi na systemie plików, co pozwala na dostęp do plików i zarządzanie nimi tak, jakby były przechowywane lokalnie.
3. Elastyczność w konfiguracji: NFS w Proxmox jest łatwy w konfiguracji. Można skonfigurować wiele zdalnych serwerów NFS

i montować ich zasoby na różnych węzłach w klastrze Proxmox.

4. Wysoka dostępność i wydajność: Współdzielenie danych poprzez NFS może zapewnić wysoką dostępność i wydajność, szczególnie w przypadku stosowania szybkich sieciowych połączeń i optymalnej konfiguracji serwerów NFS.

CEPH

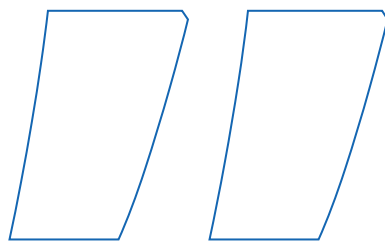
Ceph jest używany jako magazyn danych dla maszyn wirtualnych i kontenerów w Proxmox, zapewniając skalowalne, niezawodne i wysokowydajne przechowywanie danych. Oto główne cechy i zalety Ceph w Proxmox:

Rozproszona architektura: Ceph wykorzystuje rozproszoną architekturę, która umożliwia przechowywanie danych na wielu węzłach (node'ach) w klastrze. Dzięki temu zapewnia wysoką niezawodność i odporność na awarie poprzez replikację danych.

Elastyczność: Ceph jest bardzo elastycznym systemem, który pozwala na dynamiczne dodawanie nowych węzłów do klastra w celu zwiększenia przestrzeni dyskowej i wydajności przechowywania danych. Można łatwo dostosować infrastrukturę przechowywania do zmieniających się potrzeb.

Wysoka wydajność: Ceph oferuje wysoką wydajność dzięki równoległemu dostępowi do danych na wielu węzłach. To sprawia, że jest idealny do obsługi dużych obciążeń I/O, które są typowe dla środowisk wirtualizacyjnych.

Integracja z Proxmox VE: Proxmox VE oferuje wbudowaną integrację z Ceph, co ułatwia konfigurację



ZA POMOCĄ ISCSI MOŻLIWE JEST CENTRALNE ZARZĄDZANIE ZASOBAMI DYSKOWYMI POPRZECZ UDOSTĘPNIENIE JEDNEGO LUB KILKU SERWERÓW ISCSI W KLASTRZE PROXMOX. DZIĘKI TEMU MOŻNA EFEKTYWNIE ZARZĄDZAĆ PRZESTRZENIĄ DYSKOWĄ

i zarządzanie przechowywaniem danych. Można łatwo skonfigurować Ceph jako magazyn danych dla maszyn wirtualnych i kontenerów w Proxmox.

Snapshoty i replikacje: Ceph oferuje zaawansowane funkcje, takie jak migawki (snapshots) i replikacje, co

umożliwia wykonywanie kopii zapasowych danych oraz zapewnienie wysokiej dostępności.

Wirtualne dyski RBD: Ceph może być używany jako magazyn danych dla wirtualnych maszyn Proxmox poprzez wirtualne dyski RBD (RADOS Block Device), które są dynamicznie alokowane z puli zasobów Ceph. To umożliwia efektywne wykorzystanie zasobów dyskowych i elastyczne zarządzanie nimi.

iSCSI

iSCSI (Internet Small Computer System Interface) to protokół pozwalający na udostępnianie blokowych urządzeń pamięci masowej (takich jak dyski twarde i macierze RAID) przez sieć, co umożliwia wirtualnym maszynom dostęp do tych zasobów jako lokalnych urządzeń blokowych. Jest to najpopularniejsze rozwiązanie w przypadku używania macierzy dyskowych. Oto główne cechy i zalety iSCSI w Proxmox:

Wirtualizacja urządzeń blokowych: iSCSI umożliwia udostępnianie blokowych urządzeń pamięci masowej wirtualnym maszynom jako lokalne urządzenia blokowe, co pozwala na ich wykorzystanie jako dysków twardych lub macierzy RAID wewnątrz maszyn wirtualnych.

Centralne zarządzanie zasobami: Za pomocą iSCSI możliwe jest centralne zarządzanie zasobami dyskowymi poprzez udostępnienie jednego lub kilku serwerów iSCSI w klastrze Proxmox. Dzięki temu można efektywnie zarządzać przestrzenią dyskową i zapewnić dostępność danych dla wszystkich maszyn wirtualnych.

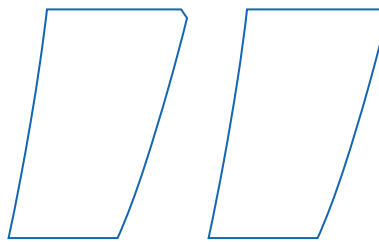
Wysoka wydajność: iSCSI oferuje wysoką wydajność dzięki bezpośredniemu dostępowi do blokowych urządzeń pamięci masowej przez sieć. To sprawia, że maszyny wirtualne mogą uzyskać dostęp do zasobów dyskowych z minimalnym opóźnieniem.

Wsparcie dla zaawansowanych funkcji: iSCSI obsługuje zaawansowane funkcje, takie jak migawki (snapshots) i replikacje, co umożliwia wykonywanie kopii zapasowych danych oraz zapewnienie wysokiej dostępności.

Integracja z Proxmox VE: Proxmox VE oferuje wbudowaną integrację z iSCSI, co ułatwia konfigurację i zarządzanie przestrzenią dyskową. Można łatwo skonfigurować iSCSI jako magazyn danych dla maszyn wirtualnych i kontenerów w GUI.

Podsumowanie

Jak zostało powiedziane na wstępie, w Proxmox możemy skorzystać z wielu metod przechowywania danych/maszyn wirtualnych. Wybór odpowiedniej zależy od decyzji administratora i powinien uwzględniać elementy takie jak: wydajność, bezpieczeństwo danych, skalowalność, prostota konfiguracji. Warto wspomnieć, iż Proxmox umożliwia coraz więcej możliwości pracy z magazynami danych, z poziomu GUI, jednak cały czas istnieje potrzeba posługiwania się linią komend dla bardziej zaawansowanych scenariuszy użycia.



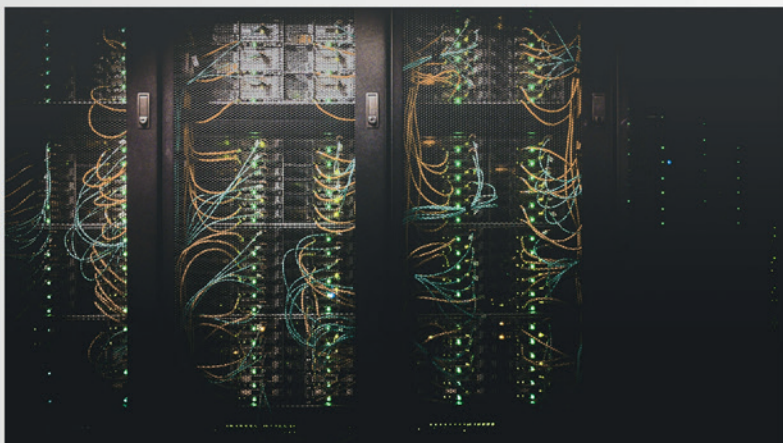
POWINIEN UWZGLĘDNIĄĆ ELEMENTY TAKIE JAK: WYDAJNOŚĆ, BEZPIECZEŃSTWO DANYCH, SKALOWALNOŚĆ, PROSTOTA KONFIGURACJI



Profesjonalne szkolenie Proxmox

22-25 PAŹDZIERNIKA 2024, Warszawa

Możliwość uzyskania dofinansowania
w ramach **KFS**



MikroTik Warsaw
Training Center

info@mwtc.pl
<https://mwtc.pl>



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