ISPROFESSIONAL

ISSN: 2449-5581

#8 (CZERWIEC 2024)

Niełatwa, choć lekko podana, refleksja nad CYFRYZACJĄ

WWW.EPIX.NET.PL

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

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

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

W naszych OpenPeeringach, kosztujących już od kilkudziesięciu złotych, oddajemy Wam już znacznie ponad połowę Internetu. Realizujemy bezpośredni dostęp do międzynarodowych operatorów: Arelion (d.Telia), Lumen, Liberty Global, GTT, Hurricane Electric i Telecom Italia Sparkle, w cenach hurtowych. Zapewniamy prosty i tani dostęp do treści pozostałych polskich IX-ów w ramach jednej usługi – Polmix, dokładnie tyle, ile potrzebujesz, bez płacenia za porty i niewykorzystane pasmo. Agregujemy ogólnopolskie zakupy ISP, wolumenu usług międzynarodowych, polskich i transmisji danych – regularnie obniżamy ceny. Posiadając port w EPIX, masz dostęp do wszystkich integratorów IPTV i dostawców innych usług. Natomiast Projekt TeleSynergia zainicjowaliśmy we współpracy z Beyond.pl, dostawcą zielonych i najbezpieczniejszych usług data center i cloud w Europie, umożliwiając dostęp kolejnym operatorom międzynarodowym do EPIX oraz poprawiając bezpieczeństwo przesyłu danych. Korzystają na tym nasi klienci.

800+ UCZESTNIKÓW

3.0 Tb/s+ RUCHU IP

1300+ PORTÓW

MiSOT GRUPA

OD REDAKCJI

AUTOR
Redakcja

Szanowni Czytelnicy,

Witamy w czerwcowym wydaniu ISProfessional! Przełomowe zmiany, które obserwujemy w branży telekomunikacyjnej, dają nam powód do refleksji nad przyszłością, która jawi się zarówno ekscytująco, jak i pełna wyzwań. Przemiany te mają fundamentalne znaczenie nie tylko dla operatorów telekomunikacyjnych, ale również dla całego społeczeństwa, które coraz bardziej polega na nowoczesnych technologiach komunikacyjnych.

Bezpieczeństwo danych, prywatność użytkowników oraz kwestie związane z cyberbezpieczeństwem stają się kluczowymi tematami, które muszą być priorytetowo traktowane. Operatorzy telekomunikacyjni muszą inwestować w nowoczesne systemy zabezpieczeń i stale aktualizować swoje procedury, aby sprostać rosnącym zagrożeniom.

Na łamach tego wydania ISProfessional przyjrzymy się bliżej tym fascynującym tematom. Eksperci z branży podzielą się swoimi spostrzeżeniami i przewidywaniami dotyczącymi przyszłości telekomunikacji. Odkryjemy, jakie innowacje czekają nas w najbliższych latach i jakie kroki należy podjąć, aby sprostać nowym wyzwaniom.

Zachęcamy do lektury i zapraszamy do dyskusji na temat przyszłości branży telekomunikacyjnej. Razem możemy lepiej zrozumieć, jakie zmiany nas czekają i jak możemy się do nich przygotować.

Życzymy inspirującej lektury!
Redakcja ISProfessional

Projekt ISProfessional #8 (czerwiec 2024) wydany w czerwcu 2024 r. realizowany jest pod patronatem Grupy MiŚOT.
Redakcja i wydawca nie ponoszą odpowiedzialności za publikowane treści. Prezentowane poglądy i opinie są opiniami danej osoby i redakcja w żaden sposób nie utożsamia się z nimi

~~~~~~

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

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

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

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

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

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

Kontakt z redakcją:
prasa@misot.pl

Nr w rejestrze wydawnictw:
PR2614

Międzynarodowy znak informacyjny:
ISSN 2449-5581

Redaktor naczelny:
Krzysztof Fujarski

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

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

Redakcja:
Paweł Gniadek
Marek Nowak
Klaudia Wojciechowska

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

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

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

Korekta:
Małgorzata Kościcka

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

Spis treści

Produkty marki cudy

w XBEST.pl
fibre optic cables & accessories

Nowoczesne rozwiązania sieciowe dla domu i biura

Technologia
Wi-Fi6

WHOLE HOME
MESH

Transmisja
2.5Gbps

Superszybkie Wi-Fi
AX3000

Tryb CCTV/VLAN
zasięg do 250m

Do 30W
na port PoE+

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

AUTOR
Marek Nowak

Niełatwa, choć lekko podana, refleksja nad cyfryzacją

Refleksji nad trzema dekadami cyfryzacji w Polsce nie da się ująć jednym zdaniem. Na Zjeździe MiŚOT w Janowie Podlaskim próbowaliśmy, wraz z przedstawicielami organizacji branżowych, ująć ją w niespełna godzinę, ale i tak pozostał niedosyt. Nasze rozmowy przed i po panelu mogłyby zaś zainspirować niejedno opracowanie naukowe z zakresu zarządzania, ekonomii i nauk politycznych. Zapraszam naukowców do kontaktu, sam przyjmuję tu ton lżejszy, by moje rozważania dało się przyswoić podczas słonecznej, mam nadzieję, majówki.

Pierwszym wątkiem dotyczącym małych i średnich operatorów telekomunikacyjnych w Polsce, którym zaskoczeni bywają teoretycy ekonomii, jest sposób prowadzenia tej działalności przed trzydziestu laty. Nasze pierwsze sieci kablowe i internetowe, począwszy od końca lat 80., rozwijały się w formie stowarzyszeń, które w istocie powoływane były w celach czysto biznesowych. Co więcej, część z nich działa w ten sposób po dziś dzień. Szerzej mówił o tym w Janowie Podlaskim Paweł Wołoch, prezes zarządu Związku Telewizji Kablowych w Polsce. Całe nagranie ze zjazdowego panelu zamieszczamy na końcu niniejszego tekstu, więc aby się tu nie powtarzać, w felietonowej formule pozwolę sobie wyrazić opinię, że często nie miało to logicznego sensu, a i podstawa prawna była naciągana.

Co więcej, jak wykazał mój pierwszy panelowy rozmówca, wszystko to działało jedynie dlatego, że nikt jeszcze nie wymyślił szeregu obowiązków, które dziś wykonują operatorzy. Mowa tu w szczególności o tych

związanych ze sprawozdawczością, a od siebie dodam także konieczność posiadania kancelarii tajnej oraz czające się za horyzontem kolejne kwestie związane z cyberbezpieczeństwem wynikające z dyrektywy NIS 2, którymi regularnie straszy na naszych łamach Marcin Zemła.

Jerzy Nowicki, prezes Związku Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM, jako jeden z warunków sprzyjających rozwojowi polskiej cyfryzacji w latach 90. wskazał również opieszałość Telekomunikacji Polskiej SA, która po prostu nie nadążała za technologią i nie potrafiła szybko się rozwinąć. Trudno temu zaprzeczyć. Moje osobiste wspomnienie z tamtego okresu to rozmowa z bliską rodziną, która po napisaniu odpowiedniego podania, miała wyznaczony termin podłączenia telefonu stacjonarnego za lat piętnaście (około dwa tysiące któregoś roku). Nie spodziewaliśmy się wówczas tak powszechnych i tanich usług z zakresu telefonii komórkowej i internetu, ani tego, że za kilka lat moja ciotka z koleżanką będą trollować chłopców na chatach młodzieżowych (nigdy nie wiesz, kto jest po drugiej stronie).

Czas interwencji

Dziki, czy jak wolą niektórzy, organiczny rozwój cyfryzacji nie mógł trwać wiecznie. I bardzo dobrze! Wie o tym każdy, kto składał w latach 90. reklamację telefonu lub był straszony kilkutysięcznymi karami za zerwanie umowy. Jest dla mnie oczywiste, że operatorzy – szczególnie komórkowi – nadużywali wówczas swojej pozycji rynkowej. Jako dziennikarz piszący w latach 90. porady dla użytkowników końcowych regularnie rozmawiałem między innymi z rzecznikami praw konsumentów i miałem szeroki obraz tych problemów. Pewne regulacje były konieczne.

NASZE PIERWSZE SIECI KABLOWE I INTERNETOWE, POCZĄWSZY OD KOŃCA LAT 80., ROZWIJAŁY SIĘ W FORMIE STOWARZYSZEŃ, KTÓRE W ISTOCIE POWOŁYWANE BYŁY W CELACH CZYSTO BIZNESOWYCH

Dziki, czy jak wolą niektórzy, organiczny rozwój cyfryzacji nie mógł trwać wiecznie.

Pojawiają się tu jednak kolejne kwestie: do jakiego stopnia należy regulować rynek, kiedy rozsądnie jest owe regulacje wyhamować, ile jeszcze przedsiębiorcy mogą ich wytrzymać i kto ma w ich imieniu krzyczeć, że już nie wytrzymują.

– Sukcesem jest to, że jest nas tak dużo, bo ponad trzy tysiące – powiedział Jerzy Nowicki w Janowie Podlaskim. – To my tworzyliśmy standardy telekomunikacji w Polsce. Nasza liczba to jednak także minus, bo nie potrafimy ze sobą rozmawiać.

A tu nie dość, że rozmawiać trzeba ze sobą, to jeszcze z administracją państwową, a budżetu na solidny lobbing po prostu nie ma. Tu także rysuje się ciekawy temat pracy naukowej z zakresu zarządzania: jak powinny funkcjonować i skąd brać finanse na swoją działalność izby gospodarcze reprezentujące przedsiębiorców. Może przynależność do nich powinna być obowiązkowa?

Większe możliwości finansowe mają, rzecz jasna, duzi rynkowi gracze, którzy nie dość, że silnie lobbują, mogą też punktowo atakować lokalnych operatorów. Paweł Wołoch osobiście prowadził sprawy przeciwko nim i gdyby nie sprawnie działające instytucje (Urząd Ochrony Konkurencji i Konsumentów oraz sądy), byłoby znacznie gorzej.

Adam Kossowski wskazał też, że pewne przekształcenia na rynku stały się konieczne. Aby starać się o pożyczki, czy szerzej – o kapitał na inwestycje, lepiej być przedsiębiorcą (na przykład spółką) niż stowarzyszeniem.

Komunikacja wewnątrz telekomunikacji

Warto też przy okazji wspomnieć o problemach komunikacyjnych między operatorami i wewnątrz organizacji ich zrzeszających.

– Telepatia nie działa – przypomniała Kinga Pawłowska-Nojszewska z Krajowej Izby Komunikacji Ethernetowej. – Czasem spotykam się z zarzutami, że jako KIKE nie reagujemy na problemy, których nikt nam wcześniej nie zasygnalizował.

Na pozdrowienia ze zjazdowej sceny zasłużył natomiast rzecznik małych i średnich przedsiębiorców Adam Abramowicz, którego wkład we wsparcie konkretnych spraw i orzeczeń odnotowała także Kinga Pawłowska-Nojszewska, Paweł Wołoch podkreślił zaś, że powołane przez rzecznika rady: przedsiębiorców, naukowa i szereg konsultacyjnych, działają także pozytywnie na rzecz integracji środowiska.

Urzędnik przedsiębiorcy nie rozumie

Stosunkowo nowa w polskim systemie prawnym instytucja rzecznika jest też wyjątkowa pod względem zrozumienia problemów, którymi się zajmuje. Adam Abramowicz, który niebawem kończy już swoją kadencję, był niegdyś przedsiębiorcą! To prawdziwa rzadkość w administracji.

– Boję się, że naszym kolejnym rzecznikiem zostanie urzędnik, który nie ma pojęcia o prowadzeniu biznesu – wspomniał Adam Kossowski z Grupy MiŚOT, wymieniając przy tej okazji listę ministrów cyfryzacji, wśród których rzeczywiście trudno znaleźć kogoś, kto miał wykształcenie w jakikolwiek sposób związane z telekomunikacją lub technologiami informacyjnymi. Mówiąc dokładniej – był taki jeden.

Tu pojawia się kolejny wątek, także nadający się na pracę naukową – kwestia kompetencji i wiedzy przedstawicieli administracji państwowej a rzeczywistość. Doświadczenie przedstawicieli przedsiębiorców branży telekomunikacyjnej wskazuje, że obecny system

STOSUNKOWO NOWA W POLSKIM SYSTEMIE PRAWNYM INSTYTUCJA RZECZNIKA JEST TEŻ WYJĄTKOWA POD WZGLĘDEM ZROZUMIENIA PROBLEMÓW, KTÓRYMI SIĘ ZAJMUJE

kształcenia kadry urzędniczej nie przygotowuje nikogo do prowadzenia dialogu z przedsiębiorcami.

– Problem ten jest systemowy – potwierdziła Kinga Pawłowska-Nojszewska, wspominając przy tym edukacyjną rolę izb w kontakcie z politykami. Wielu z nich po prostu należy na wstępie tłumaczyć, jak wygląda polski rynek telekomunikacyjny.

Z drugiej jednak strony, gdy zaproponowałem, by kogoś z aktywnych przedstawicieli przedsiębiorców w Grupie MiŚOT wysłać do ministerstwa, Adam Kossowski (nie słychać tego na nagraniu) spontanicznie zripostował: Chyba za karę. Główny trend wędrówek jest więc inny, choć przepływy zdarzają się w obie strony, a lokalnych polityków i polityczki można spotkać także w Grupie MiŚOT.

AUTOR
Marek Nowak

IDC CIO Summit – relacja

Na sopockim spotkaniu CIO, czyli dyrektorów do spraw informacji z różnych sektorów gospodarki, prezentowano najnowsze trendy w cyfryzacji. Dużo miejsca poświęcono praktycznemu wykorzystaniu sztucznej inteligencji, nie zabrakło też tematów związanych z cyberbezpieczeństwem i smart city.

CIO, czyli Chief Information Officer to osoba odpowiedzialna w organizacji za stan, rozwój i wdrożenia technologii informacyjnych. Jest to funkcja szczególnie ważna w erze cyfryzacji. Jeszcze niedawno działania CIO ograniczały się głównie do zarządzania infrastrukturą informatyczną lub teleinformatyczną oraz zapewniania wydajności systemów. Dzisiejsi dyrektorzy do spraw informacji (lub informatyki – nazewnictwo bywa tu różne) stali się kluczowym elementem strategii biznesowych.

Oczywiście w przypadku małych i średnich operatorów telekomunikacyjnych często nie ma nawet tak wyodrębnionego stanowiska (funkcję tę pełni właściciel, jeden ze wspólników lub członków zarządu), warto jednak poznać perspektywę ludzi, którzy specjalizują się w tej właśnie dziedzinie.

Cyfrowe trendy usług publicznych

Pierwszy blok merytoryczny IDC CIO Summit skupił się na punktach przecięcia pomiędzy technologią a usługami publicznymi. Nie sposób mówić o tych zagadnieniach bez położenia silnego akcentu na kwestię cyberbezpieczeństwa. Trudno byłoby bez tego namówić użytkowników do korzystania z serwisów. Z drugiej strony każdemu z nas zależy na tym, by z aplikacji urzędowych korzystać szybko, sprawnie i w jak najbardziej intuicyjny sposób.

Centralnym elementem usług publicznych w Polsce jest mObywatel. To bezpłatna, publiczna aplikacja mobilna, dzięki której możemy uzyskać szybki dostęp do swoich dokumentów i danych. Aplikacja wciąż się rozwija i dodawane są do niej kolejne funkcje, zyskała też ogromną popularność.

Radosław Maćkiewicz z Centralnego Ośrodka Informatyki, który jest odpowiedzialny za sprawne funkcjonowanie mObywatela, podkreślił, że zdalna administracja wychodzi od zadania pytań: *Po co to robimy?* oraz *Komu i do czego to ma służyć?*

– Praktycznie codziennie obserwujemy testowanie naszych systemów – zaznaczył w swej wypowiedzi.

– Musimy pamiętać, że nasi przeciwnicy, a często są to hakerzy działający pod egidą służb specjalnych określonych państw, wykorzystują technologię przeciw nam – podkreślał generał dywizji Karol Molenda, dowódca Komponentu Wojsk Obrony Cyberprzestrzeni. – Widzimy na co dzień, jak próbują wpływać na nasze systemy obronne. Uważam też, że tak samo ważne jak nasze przygotowanie, jest budowanie świadomości zagrożeń u obywateli. Niezwykle ważna jest cyberhigiena.

– Konieczna jest współpraca, wymiana wiedzy i reaktywność, szczególnie gdy pojawiają się nowe wektory ataku – dodał Marcin Grabarczyk, dyrektor Pionu Transferu Technologii i Rozwoju Biznesu NASK-PIB.

– Nie daje mi zasnąć jedynie cisza – podkreślił Karol Molenda. – Odpieranie kolejnych cyberataków jest codziennością, gdy ich nie ma, to znaczy, że albo czegoś nie wiemy, albo przeciwnik przygotowuje się do czegoś większego.

Podczas dyskusji przytoczono także kilka przykładów z wojny w Ukrainie, gdzie aplikacje podobne do mObywatela pomagają także w sygnalizowaniu zagrożeń i przekazywaniu informacji o ruchach wojsk nieprzyjaciela.

Polskie smart city

W kolejnym interesującym nas panelu, tym razem dotyczącym rozwiązań z zakresu smart city, udział wzięli przedstawiciele Sopotu, Koszalina, Warszawy i Poznania. Oprócz znanych już naszym stałym Czytelnikom stołecznych rozwiązań, Michał Olszewski, zastępca Prezydenta m.st. Warszawy, przypomniał o przetargu, w wyniku którego ma pojawić się na stołecznych latarniach 120 tys. punktów transmisji danych 5G. Kolejnym krokiem będzie też wprowadzenie na warszawskich przystankach komunikacji miejskiej rozkładów jazdy wyświetlanych na e-papierze.

W toku dyskusji wskazano też interesujące inicjatywy lokalne, wynikające z potrzeb konkretnych miejscowości.

– Dużo czerpiemy z pomysłów warszawskich, jak na przykład w kwestii podłączeń nowych śmietników, które przekazują informacje o stanie swojego wypełnienia. Mamy też projekty własne wychodzące naprzeciw

problemom, z którymi się stykamy – mówiła Magdalena Cieślik, przewodnicząca zespołu ds. wdrażania innowacji i rozwoju miasta w koncepcji smart city sopockiego Urzędu Miasta. Jako przykłady takich rozwiązań wskazała opaskę pozwalającą rodzicom szybciej odnajdywać dzieci, które zgubiły się na plaży oraz aplikację parkingową funkcjonującą w tutejszej marinie, dzięki której lepiej zarządza się miejscami postojowymi.

– Z naszego doświadczenia wynika, że wprowadzając rozwiązania smart city, warto od początku myśleć o mieście jako całości i unikać wysp rozproszonych inwestycji – podpowiadał Michał Łakomski, pełnomocnik Prezydenta Miasta Poznania ds. Smart City.

Przedstawiciele administracji samorządowej zgodnie podkreślali też, że rozwiązania smart opłacają się oraz, że warto prowadzić dialog techniczny z przedstawicielami rynku.

Cyberbiznes

Kolejne wystąpienia podczas dwóch intensywnych dni IDC CIO Summit skupiały się na wprowadzaniu cyfrowych rozwiązań do biznesu. Wyłonił się stąd obraz, że dyrektorzy ds. informacji wykorzystują dziś innowacje w kształtowaniu strategicznych kierunków organizacji, tworzeniu wartości oraz zwiększaniu dochodów firmy. Wielu z nich wdraża już także rozwiązania oparte na sztucznej inteligencji.

UWAŻAM TEŻ, ŻE TAK SAMO WAŻNE JAK NASZE PRZYGOTOWANIE, JEST BUDOWANIE ŚWIADOMOŚCI ZAGROŻEŃ U OBYWATELI. NIEZWYKLE WAŻNA JEST CYBERHIGIENA

Praktyczne rozwiązania tego pojawiają się już w analizie Big Data, logistyce, gamingu, obsłudze klientów, diagnostyce medycznej (a pioniersko nawet w operacjach chirurgicznych). Coraz częściej korzystamy też z rozwiązań chmurowych.

– Cyfrowa transformacja dla każdego oznacza dziś co innego – wskazał Marc Dowd, doradca IDC, obsługujący dyrektorów ds. informatyki w przedsiębiorstwach o wartości wielu miliardów euro. – Ze względu jednak na spodziewaną w najbliższym czasie recesję, możemy się założyć, że zwolnią długofalowe inwestycje w technologie i skupimy się na tych, które dadzą rezultaty jeszcze w tym roku. Dla cyfryzacji ważne są w związku z tym: jasna komunikacja, celowość i wskazanie korzyści.

AUTOR
Marek Nowak

Centrum Przetwarzania Danych Grupy MiŚOT

Stan prac

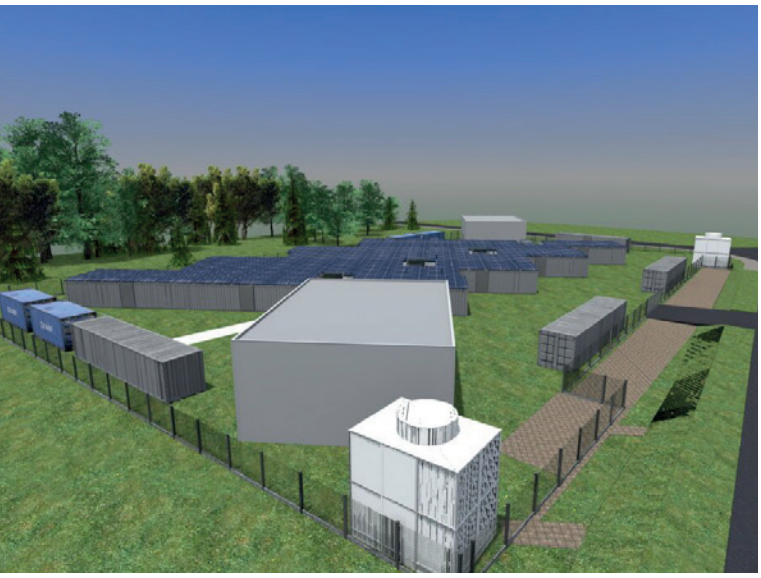
Mijają dwa lata od rozpoczęcia budowy nowoczesnego Centrum Przetwarzania Danych Grupy MiŚOT. Powstaje ono na Śląsku, w Jaworznie. Przedstawiamy najnowszy raport z budowy.

W maju 2022 roku Grupa MiŚOT kupiła grunt w strefie przemysłowej w Jaworznie z zamiarem wybudowania tam nowoczesnego Centrum Przetwarzania Danych. Powstające budynki będą także stanowić zaplecze dla dalszego rozwoju węzła wymiany ruchu EPIX. Inwestycja szacowana jest na kilkanaście milionów złotych.

Przedstawiciele inwestorów zapewniają, że Centrum Przetwarzania Danych będzie bardzo nowoczesną i innowacyjną jednostką, zapowiadają też, że zaskoczą branżę wieloma rozwiązaniami z obszaru technologii i ochrony środowiska.

Co już się wydarzyło?

Lista już wykonanych prac jest długa. Obejmuje projekty budowlane i zagospodarowania terenu, a także projekt zjazdu z drogi miejskiej na teren przyszłego Data Center (uzyskano w tym zakresie zgodę i podpisano umowę z Urzędem Miasta), dokumentację geologiczno-inżynierską oraz wypełnienie szeregu obowiązków związanych z geodezją.



WYZWANIEM BYŁY TEŻ PRACE ZWIĄZANE Z PRZYŁĄCZEM PRĄDU POCZĄWSZY OD PRZYGOTOWANIA I UZGODNIENIA PROJEKTU UKŁADU POMIAROWEGO ŚREDNIEGO NAPIĘCIA

Wyzwaniem były też prace związane z przyłączem prądu począwszy od przygotowania i uzgodnienia projektu układu pomiarowego średniego napięcia. Wybudowano już linię SN, ułożono kable w ziemi pomiędzy stacją TAURON, a budynkiem energetycznym nr 1, podpisano umowę przyłączeniową, a także wybudowano przyłącze budowlane i podpisano umowę na dostawę energii. Zakupiono transformator 400kVA na potrzeby uruchomienia zasilania SN.

Wykonano także przyłącze wody i podpisano umowę na dostawę wody z Wodociągami Jaworzno.

Projekt budowy kanalizacji telekomunikacyjnej podzielony został na trzy etapy. Uzyskano zgody na jej wykonanie, a następnie wykonano kanalizację telekomunikacyjną z etapu 1 i 2 od DC do ulicy Emilii Plater. Wykonano przyłącze światłowodowe do AC celem podłączenia systemów bezpieczeństwa z budowy i umożliwienia zdalnego nadzoru.

Wykonano projekt architektoniczno-konstrukcyjny budynku energetycznego nr 1 z serwerownią oraz projekt techniczny instalacji elektrycznej nN i SN dla budynku energetycznego nr 1 z serwerownią.,

Ogrodzono i oczyszczono teren budowy, a także uruchomiono na nim alarm i monitoring CCTV, który obejmuje zarówno teren magazynowy, jak i teren samej budowy.

Wykonano ściany EI30 w dwóch kontenerach przeznaczonych na serwerownie chłodzone powietrzem, przygotowano ruszty pod sufity, wykonano okablowanie na potrzeby instalacji elektrycznych i teletechnicznych w tych kontenerach. Przeprowadzono też prace konserwacyjne i porządkowe na terenie zaplecza.

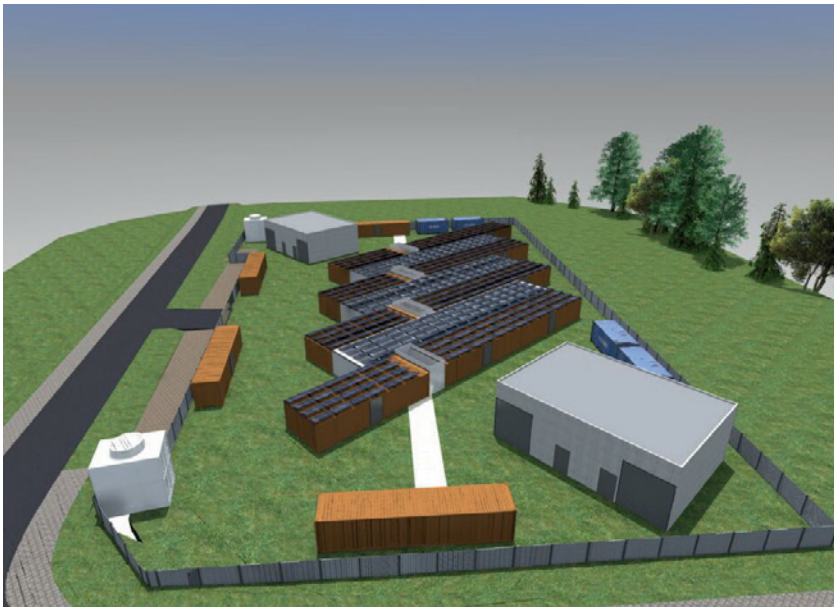
Na terenie budowy przygotowano już także drogę z przeznaczeniem docelowym i wybrano wykonawcę pierwszego budynku (umowy z inspektorem nadzoru i kierownikiem budowy także są już podpisane).

Co dzieje się aktualnie?

Projekt budowlany budynku energetycznego nr 2 z serwerownią jest już złożony do Urzędu Miasta i procedowane jest wydanie zezwolenia na jego budowę. Podobna sytuacja ma miejsce w przypadku projektu budowlanego zagospodarowania terenu DC dla budynku 2 i projektu wykonawczego zatok postojowych na terenie miasta.

Nadal trwa też szereg prac projektowych. Przygotowywane są projekty techniczne instalacji sanitarno-wentylacyjnej dla budynków energetycznych z serwerowniami, instalacji wentylacji i chłodzenia dla 24 kontenerów, architektoniczno-konstrukcyjny dla budynku energetycznego nr 2 z serwerownią, instalacji elektrycznej nN i SN dla budynku energetycznego nr 2 z serwerownią, PZT dla 24 kontenerów, instalacji niskoprądowych dla budynku energetycznego nr 1 i 2 z serwerownią, trwa także przeprowadzka z magazynów do zaplecza budowy.

Po wypełnieniu formalności (opinia Komendy Miejskiej Policji w Jaworznie dla projektów czasowej i stałej organizacji ruchu, zgłoszenie budowy do Nadzoru Budowlanego



EKSPERCI NIE MAJĄ WĄTPLIWOŚCI, ŻE PRZYCHODY Z USŁUG DATA CENTER WZROSNĄ

w Jaworznie), można już także oficjalnie stwierdzić, że ETAP 1 budowy rozpocznie się z dniem 10.06.2024.

Dobry czas dla DC

Decyzja o budowie Centrum Przetwarzania Danych Grupy MiŚOT zapadała, gdy ruch w sieci EPIX przekraczał trzy Terabity na sekundę, a w trzech naszych węzłach (Katowice, Warszawa i Poznań) obsługiwanych było już ponad 850 klientów.

Analizy rynku centrów danych w Polsce i prognozy jego rozwoju na najbliższe lata wskazują, że zapotrzebowanie na usługi kolokacji będzie rosnąć, pojawią się także nowi odbiorcy zagraniczni. Rozwój zaś doprowadzi do większego podziału rynku na część hurtową i detaliczną. Eksperci nie mają wątpliwości, że przychody z usług data center wzrosną. Będzie mieć na to wpływ postępująca koncentracja kapitału w Polsce, ale również nowi inwestorzy pojawiający się w naszym kraju.

Już w 2021 roku firma PMR wykazała w swym raporcie, że do 2025 roku jego zasoby mogą się podwoić. Nie brakuje także inwestycji zagranicznych w tym sektorze. W Warszawie inwestuje także amerykański Netskope, duże plany ma także Data4 – operator i inwestor rynku centrów danych z Francji.

AUTOR
Michał Koch

Ministerstwo Cyfryzacji obiecuje KSC w przeciągu roku

Ministerstwo Cyfryzacji przedstawiło nowy projekt ustawy dotyczącej krajowego systemu cyberbezpieczeństwa. Regulacje są niezbędne zwłaszcza teraz, gdy liczba incydentów dotyczących cyberbezpieczeństwa stale wzrasta.

Na spotkaniu w ministerstwie poruszono tematy Dyrektywy NIS 2, Toolbox 5G (środki dotyczące minimalnej harmonizacji w ramach UE) oraz Krajowego Planu Odbudowy i Zwiększania Odporności cyfrowej infrastruktury kraju. Minister cyfryzacji Krzysztof Gawkowski przedstawił rys dotyczący tego zagadnienia na najbliższe miesiące. Przepisy mają być też pełną implementacją Dyrektywy NIS 2.

– Chcemy tę ustawę w końcu przeprowadzić. Mówimy o kolosalnej zmianie dla państwa. Potrzebne będą olbrzymie pieniądze z budżetu na cyberbezpieczeństwo – stwierdził minister Gawkowski.

Krajowy system cyberbezpieczeństwa, zgodnie ze słowami ministra, to kluczowa kwestia dla bezpiecznej przyszłości kraju. Każdy dzień zwłoki to droga donikąd. Implementacja przepisów planowana jest w ciągu najbliższego roku. Ustawa ma być przeprocesowana do końca grudnia, a podmioty na dostosowanie stanu faktycznego do nowych przepisów będą miały sześć miesięcy.

W przygotowanych przepisach brak jest instytucji operatora strategicznego. Ten podmiot ma być wprowadzony odrębną ustawą.

Projekt ustawy KSC to dopiero pierwszy krok do zwiększenia bezpieczeństwa kraju. Wiceminister Paweł Olszewski zaznaczył, że ministerstwo planuje szeroko zakrojone konsultacje z podmiotami obecnymi na rynku.

– To kwestia wizualizacji zagrożeń, zwłaszcza że realia są takie, że w Ukrainie trwa wojna. Zdajemy sobie sprawę, że pracy jest sporo, a wyzwania stoją przed wszystkimi podmiotami na rynku. Nikogo nie chcemy jednak wykluczać. Zależy nam, aby krajobraz bezpieczeństwa był przejrzysty. Bezpieczeństwo ma pierwszeństwo.

Co z wymianą sprzętu wysokiego ryzyka? Minister Gawowski przyznał, że przepisy nie są wymierzone w żadne konkretne przedsiębiorstwa. Założeniem tego działania ma być przede wszystkim naprawa regulacji w praktyce. Kary będą wyznaczone zgodnie z parametrami zawartymi w ustawie. Dla podmiotów kluczowych kary wyniosą 10 mln PLN. Wymiana będzie musiała odbyć się w ciągu 7 lat (4 lata w przypadku sektorów

krytycznych). Koszt wymiany nie będzie zwracany podmiotom z budżetu kraju.

Warto też odnotować, że Minister Cyfryzacji będzie informował prokuratora generalnego, że takie naruszenie zostało stwierdzone, a w procesie udział będzie brało Kolegium ds. Cyberbezpieczeństwa. Dostawca usług internetowych będzie mógł odwołać się od decyzji administracyjnej.

– Ustawę piszemy dla bezpieczeństwa Polski. Nie sposób nie brać pod uwagę obecnej geopolityki – dodał minister Gawkowski.

Przepisy KSC zawierają też instrument polecenia zabezpieczającego. Podkreślono, że ma to być narzędzie, które nie blokuje internetu, ale służy w incydentalnych przypadkach, gdy mają miejsce krytyczne podatności. Polecenie będzie wydawane przez ministra cyfryzacji w formie decyzji.

Wiceminister Olszewski zaznaczył, że czas nagli: – Tak naprawdę to dziś startujemy z wdrażaniem KSC. Nadrabiamy stracony czas, gdyż te przepisy powinny być wdrożone już dawno temu. Problem jest jednak realny, o czym alarmują m.in. eksperci z NASK.

Pojawić się ma również ocenia poziomu bezpieczeństwa, które będzie weryfikowane przez jednostki zajmujące się zarządzaniem bezpieczeństwem (m.in. CSIRT).

Wśród planów jest również wprowadzenie programu Bezpieczny Samorząd, który odnosi się do zwiększania świadomości urzędników jednostek samorządu terytorialnego. Minister Gawkowski skrytykował również opieszałość poprzedniej władzy, która nie zrealizowała obietnic dotyczących cyberbezpieczeństwa i standaryzacji.

Projekt ustawy został opublikowany. Konsultacje publiczne potrwają do 24 maja 2024 r.

ZDAJEMY SOBIE SPRAWĘ, ŻE PRACY JEST SPORO, A WYZWANIA STOJĄ PRZED WSZYSTKIMI PODMIOTAMI NA RYNKU. NIKOGO NIE CHCEMY JEDNAK WYKLUCZAĆ. ZALEŻY NAM, ABY KRAJOBRAZ BEZPIECZEŃSTWA BYŁ PRZEJRZYSTY. BEZPIECZEŃSTWO MA PIERWSZEŃSTWO

CYBERBEZPIECZEŃSTWO

AUTOR
Michał Koch

Wzrost liczby zagrożeń

W 2023 roku zanotowano wzrost liczby nowych luk w zabezpieczeniach oprogramowania oraz urządzeń sieciowych. Stanowi to istotne wyzwanie dla bezpieczeństwa użytkowników w internecie. Zespół CERT Polska aktywnie monitoruje podatności, aby w miarę możliwości zapobiegać działaniu cyberprzestępców.

Szczególną uwagę należy zwrócić na statystyki Agencji ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (CISA), które umożliwiają dokładniejszą ocenę aktualnego krajobrazu zagrożeń. Na koniec 2023 roku aktywnie wykorzystywanych było 1074 różnych podatności, z czego 137 opublikowano w tym samym roku. Dla porównania, w roku 2022 było ich odpowiednio 868 i 92.

Zespół CERT Polska zaleca szczególnie administratorom sieci i kierownikom jednostek ciągłe śledzenie komunikatów bezpieczeństwa, które publikowane są przez producentów posiadanego oprogramowania, a także priorytetowe wykonywanie aktualizacji podatnych systemów w celu zapewnienia bezpieczeństwa organizacji.

Ważne jest bezustanne monitorowanie infrastruktury pod względem występujących anomalii, które mogłyby świadczyć o tym, że jest ona przedmiotem ataku. Ignorowanie zagrożeń związanych z krytycznymi podatnościami może skutkować incydentami bezpieczeństwa, takimi jak ataki ransomware lub wycieki danych krytycznych.

IGNOROWANIE ZAGROŻEŃ ZWIĄZANYCH Z KRYTYCZNYMI PODATNOŚCIAMI MOŻE SKUTKOWAĆ INCYDENTAMI BEZPIECZEŃSTWA, TAKIMI JAK ATAKI RANSOMWARE LUB WYCIEKI DANYCH KRYTYCZNYCH

Podatności o kluczowym znaczeniu

Microsoft Outlook (CVE-2023-23397)

Krytyczna podatność w aplikacji Outlook w systemie Windows mogła prowadzić do zdalnego przejęcia hasła domenowego bez interakcji użytkownika. Do ataku wystarczało otrzymanie przez ofiarę wiadomości e-mail zawierającej odpowiednio spreparowane wydarzenie kalendarza albo zadanie, które powodowało odwołanie do ścieżki UNC kontrolowanej przez atakującego. Podatność pozwalała na przechwycenie skrótu NTLMv2 i późniejszą próbę odzyskania hasła domenowego poprzez atak siłowy. W sytuacji, gdy atakujący miał dostęp do sieci ofiary, możliwym było również bezpośrednie wykorzystanie skrótu NTLMv2 do zalogowania w innych usługach bez potrzeby łamania, tzw. NTLM relay. W związku z tą podatnością zespół CERT Polska wysłał 4075 ostrzeżeń do różnych organizacji.

Fortigate SSL-VPN (CVE-2023-27997)

Podatność w urządzeniach Fortigate z systemem FortiOS to luka związana z przepełnieniem bufora sterty w module wstępnego uwierzytelniania usługi SSL-VPN. Jej wykorzystanie pozwalało na przepełnienie nadmiaru danych z zaalokowanego bloku pamięci do sąsiednich bloków na stercie, tym samym umożliwiając wykonanie dowolnego złośliwego kodu, nawet w przypadku, kiedy włączone było uwierzytelnianie dwuskładnikowe. Podatność została opublikowana 12 czerwca, a już 14 czerwca publicznie dostępne były exploity pozwalające na jej wykorzystanie, co zwiększało ryzyko wzmożonych ataków ransomware. Zespół CERT Polska wykrył 218 instancji usług SSL-VPN urządzeń Fortigate z systemem FortiOS w polskiej adresacji, które były podatne na CVE-2023-27997. W związku z tym wysłano 128 powiadomień do różnych organizacji.

Cisco IOS XE (CVE-2023-20198)

Podatność dotyczyła funkcjonalności Web User Interface w oprogramowaniu Cisco IOS XE, stosowanej do zarządzania systemem, opartym na graficznym interfejsie użytkownika. Atakujący miał możliwość utworzenia nowego konta administratora z poziomu interfejsu użytkownika, bez konieczności autoryzacji. Konto to służyło do utworzenia implantu zawierającego

plik konfiguracyjny cisco_service.conf. Aby implant stał się aktywny, serwer sieciowy musiał zostać ponownie uruchomiony. Sam punkt końcowy przyjmował określone parametry, które umożliwiały atakującemu wykonanie dowolnych poleceń na poziomie systemu. Zespół CERT Polska znalazł 492 instancje Cisco IOS XE w polskiej adresacji, które były podatne na CVE-2023-20198. W związku z tym wysłano 106 powiadomień do różnych organizacji.

Wycieki danych a bezpieczeństwo

Wycieki danych, czy to z powodu ataków hakerskich, nieszczelności systemów, czy po prostu nieostrożności, stały się częstym zjawiskiem. Oto kilka ważnych kwestii dotyczących tego zagadnienia:

- Źródła wycieków danych
- Wycieki danych mogą mieć różne źródła. Mogą wynikać z cyberataków, takich jak ataki hakerskie na bazy danych lub sieci korporacyjne. Mogą również wynikać z niezabezpieczonych serwerów, nieszczelności oprogramowania lub ludzkiej pomyłki, np. przekazania poufnych informacji osobie trzeciej.
- Typy danych podatnych na wyciek
  Wycieki danych mogą obejmować różne typy informacji, od danych osobowych, takich jak imiona, nazwiska, numery identyfikacyjne, po dane finansowe, medyczne, a nawet dane związane z działalnością biznesową.
- Konsekwencje dla osób i firm
  Wycieki danych mogą mieć poważne konsekwencje dla osób fizycznych i firm. Dla osób prywatnych może to oznaczać kradzież tożsamości, oszustwa finansowe lub inne formy nadużyć. Dla firm może to prowadzić do utraty zaufania klientów, sankcji prawnych, a nawet bankructwa.
- Zabezpieczenia przed wyciekami danych
  Istnieje wiele sposobów zabezpieczania się przed wyciekami danych, w tym stosowanie silnych haseł, szyfrowanie danych, regularne aktualizacje oprogramowania, przeszkolenie personelu w zakresie bezpieczeństwa cyfrowego oraz monitorowanie aktywności sieciowej w celu wykrywania potencjalnych incydentów.

W przypadku zauważenia zagrożenia ważne jest szybkie reagowanie i podejmowanie odpowiednich środków zaradczych w celu minimalizacji szkód oraz ochrony prywatności i bezpieczeństwa osób dotkniętych incydentem. Organizacje powinny również regularnie

WYCIEKI DANYCH, CZY TO Z POWODU ATAKÓW HAKERSKICH, NIESZCZELNOŚCI SYSTEMÓW, CZY PO PROSTU NIEOSTROŻNOŚCI, STAŁY SIĘ CZĘSTYM ZJAWISKIEM

przeprowadzać audyty bezpieczeństwa i aktualizować swoje procedury w celu zapobiegania przyszłym wyciekom danych.

Zwalczanie nadużyć w komunikacji elektronicznej

W ciągu ostatnich dwóch lat zespół CERT Polska intensywnie pracował nad nowym projektem legislacyjnym mającym na celu zwalczanie zagrożeń cybernetycznych. Współpracując z Ministerstwem Cyfryzacji, Urzędem Komunikacji Elektronicznej oraz firmami z sektora telekomunikacyjnego, przygotował ustawę, która ma odciążyć użytkowników od ataków phishingowych, smishingowych oraz innych form oszustw internetowych.

Efektem tych starań jest ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej.

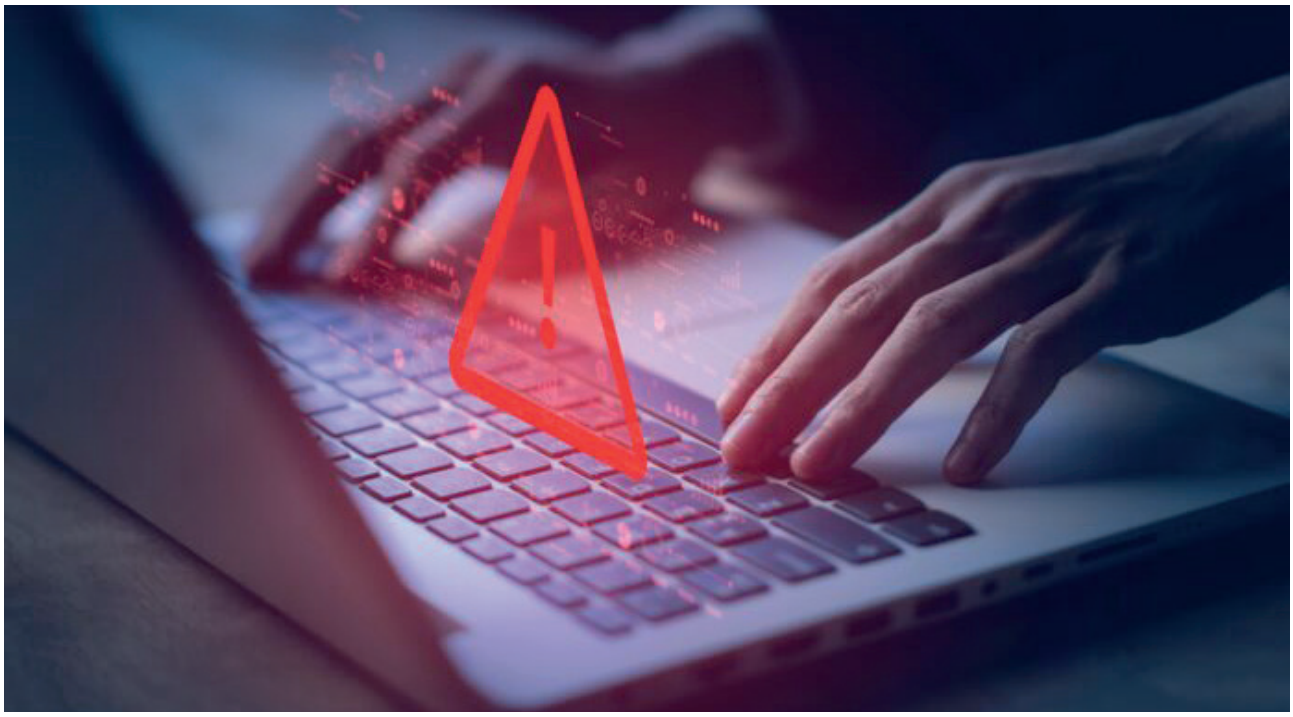
Przepisy weszły w życie 24 września, choć nie wszystkie zapisy obowiązywały już od tego momentu.

- Phishing
  W walce z phishingiem zastosowano sprawdzone autorskie rozwiązanie CERT Polska, czyli Listę ostrzeżeń. Projekt ten, istniejący od 2020 roku, powstał dzięki współpracy Ministerstwa Cyfryzacji oraz kilku operatorów telekomunikacyjnych. Wpisanie listy do ustawy umożliwia również innym operatorom korzystanie z niej, co zwiększa ochronę przed złośliwymi domenami. Skargi dotyczące blokowania domen rozpatrywane są bezpośrednio przez Prezesa Urzędu Komunikacji Elektronicznej.

- Smishing
  CERT Polska tworzy i upublicznia wzorce wiadomości smishingowych, a operatorzy telekomunikacyjni są zobowiązani blokować wiadomości, które pasują do tych wzorców. Wzorce są oparte na wyrażeniach regularnych, a system działa od kwietnia 2024 roku. Podmioty publiczne mają obowiązek korzystania z rejestru nadpisów wiadomości SMS, co ma zapewnić bezpieczeństwo użytkowników.

- Spoofing e-mail
  Podmioty publiczne muszą stosować protokoły SPF, DMARC oraz DKIM. Każdy z nich odgrywa istotną rolę w weryfikacji autentyczności nadawcy, upewniając się, że otrzymywane wiadomości są rzeczywiście wysyłane z prawidłowej domeny. W obliczu ataków cyberprzestępców te mechanizmy działają jak tarcza.

  Wdrożone regulacje obowiązują tylko sektor publiczny, jednak zachęca się również podmioty prywatne do korzystania z tych rozwiązań. Stworzono narzędzie bezpieczna-poczta.cert.pl, które ma wspierać tę inicjatywę.



- CLI spoofing
  Aby walczyć ze spoofingiem telefonicznym, opracowano rozwiązanie mające na celu blokowanie połączeń lub usuwanie zmodyfikowanych etykiet dzwoniących. Lista numerów, z których nie można wykonywać połączeń, została uruchomiona od marca 2024 roku, a pełna walka z tym zjawiskiem ma się rozpocząć najpóźniej do września 2024 roku.

Wszystkie powyższe inicjatywy mają na celu zwiększenie bezpieczeństwa użytkowników w sieci poprzez utrudnienie cyberprzestępcom działania oraz ochronę danych osobowych przed nieuprawnionym dostępem. Oczekuje się, że nowe regulacje przyniosą wymierne efekty w ograniczeniu ataków internetowych.

CERT na straży!

CERT Polska dzięki monitorowaniu, wykrywaniu i przeciwdziałaniu różnorodnym zagrożeniom internetowym odgrywa kluczową rolę

OCZEKUJE SIĘ, ŻE NOWE REGULACJE PRZYNIOSĄ WYMIERNE EFEKTY W OGRANICZENIU ATAKÓW INTERNETOWYCH

W ODPOWIEDZI NA ROSNĄCE ZAGROŻENIA CERT POLSKA ZAINICJOWAŁ NOWĄ, BARDZIEJ INTUICYJNĄ WERSJĘ LISTY OSTRZEŻEŃ ORAZ WPROWADZIŁ UŁATWIENIA W ZGŁASZANIU PODEJRZANYCH WIADOMOŚCI SMS

w zapewnianiu cyberbezpieczeństwa w naszym kraju. Instytucja ta stara się też minimalizować skutki cyberataków oraz chronić infrastrukturę i dane użytkowników.

Miniony rok był znaczącym okresem dla cyberbezpieczeństwa w Polsce. W trzecim kwartale roku weszła w życie ustawa o zwalczaniu nadużyć w komunikacji elektronicznej. W odpowiedzi na rosnące zagrożenia CERT Polska zainicjował nową, bardziej intuicyjną wersję Listy Ostrzeżeń oraz wprowadził ułatwienia w zgłaszaniu podejrzanych wiadomości SMS.

Aktywność w ramach kampanii #BezpiecznyPrzemysł

W ramach inicjatywy #BezpiecznyPrzemysł eksperci z CERT Polska kontynuowali działania mające na celu podniesienie poziomu cyberbezpieczeństwa polskiej infrastruktury przemysłowej. Narzędzie Snitch, które zostało znacząco rozbudowane, automatyzuje proces identyfikacji urządzeń przemysłowych widocznych w publicznym internecie, takich jak sterowniki PLC czy panele HMI, oraz informuje właścicieli o potencjalnych zagrożeniach.

Artemis

Artemis to narzędzie rozwijane przez zespół CERT Polska we współpracy z kołem naukowym Politechniki Warszawskiej KN Cyber, które w 2023 roku odnotowało znaczące sukcesy w zakresie poprawy cyberbezpieczeństwa w Polsce. Artemis przeskanował ponad 50,6 tys. domen i adresów IP, znajdując ponad 180 tys. podatności i błędnych konfiguracji.

Projekt skoncentrował się na badaniu stron internetowych i systemów dostępnych publicznie w poszukiwaniu błędów konfiguracyjnych i podatności, umożliwiając tym samym ich szybką identyfikację. Regularne skanowanie pozwala nie tylko na bieżące monitorowanie stanu bezpieczeństwa, ale także na jego poprawę poprzez niezwłoczne informowanie administratorów o wykrytych zagrożeniach. Co więcej, CERT Polska weryfikuje, czy wprowadzone zmiany skutecznie eliminują wykryte problemy.

Artemis nie tylko podnosi poziom bezpieczeństwa konkretnych instytucji, ale także przyczynia się do budowania szerokiego obrazu cyberbezpieczeństwa na terenie Polski. Wyniki skanowania pozwalają kierować zasoby CERT tam, gdzie są one najbardziej potrzebne, a także inicjować kampanie informacyjne i edukacyjne.

Szczególną uwagę warto zwrócić na różnorodność obszarów, które zostały objęte badaniem. Wśród przeskanowanych domen znalazły się m.in. placówki oświatowe, jednostki samorządu terytorialnego, instytucje zdrowotne, banki, a także uczelnie i domeny rządowe. Odkryto wiele krytycznych podatności, które mogłyby prowadzić do poważnych incydentów bezpieczeństwa, takich jak przejęcie kontroli nad stronami internetowymi lub dostęp do wrażliwych danych.

Równie ważne jest, że wszystkie kluczowe informacje oraz zalecenia dotyczące zabezpieczeń są udostępniane na dedykowanej stronie internetowej, co minimalizuje stres i ryzyko pochopnych działań ze strony administratorów. Kod źródłowy Artemis jest również publicznie dostępny, co umożliwia międzynarodowym zespołom CERT wykorzystanie tego narzędzia w swojej pracy, wspierając globalne wysiłki na rzecz poprawy cyberbezpieczeństwa.

Edukacja i promocja cyberbezpieczeństwa

W ostatnich miesiącach 2023 roku analitycy zajmujący się bezpieczeństwem sieci odnotowali znaczący wzrost zgłoszeń, co można przypisać skutecznym kampaniom edukacyjnym i promocyjnym. Wprowadzenie bezpłatnego numeru 8080, umożliwiającego zgłaszanie podejrzanych wiadomości SMS, miało kluczowe znaczenie. Od listopada 2023 r., kiedy to liczba zgłoszeń wynosiła około 42 tys., liczba ta wzrosła do ponad 100 tys. w grudniu, osiągając na koniec roku niemal 400 tys. zgłoszeń. Zdecydowanie wzrostowa tendencja utrzymała się również w styczniu 2024 br.

Dzięki współpracy z Ministerstwem Cyfryzacji oraz NASK-PIB zrealizowano również kampanie finansowane ze środków Unii Europejskiej, które obejmowały

ODKRYTO WIELE KRYTYCZNYCH PODATNOŚCI, KTÓRE MOGŁYBY PROWADZIĆ DO POWAŻNYCH INCYDENTÓW BEZPIECZEŃSTWA, TAKICH JAK PRZEJĘCIE KONTROLI NAD STRONAMI INTERNETOWYMI LUB DOSTĘP DO WRAŻLIWYCH DANYCH

Zdecydowanie wzrostowa tendencja utrzymała się również w styczniu 2024 br.

KOLEJNYM WYZWANIEM JEST PRZEKONANIE PRYWATNYCH WŁAŚCICIELI DO PODJĘCIA DZIAŁAŃ ZABEZPIECZAJĄCYCH, CO NIE ZAWSZE JEST MOŻLIWE ZE WZGLĘDU NA BRAK OBOWIĄZKU LUB UMIEJĘTNOŚCI TECHNICZNYCH

emisję spotów telewizyjnych i radiowych, a także szeroko zakrojone działania w social mediach. Kampanie te nie tylko zwiększyły rozpoznawalność zagrożeń cybernetycznych wśród Polaków, ale także wzmocniły zaufanie do działalności CERT Polska jako wiarygodnego źródła wsparcia w sytuacjach zagrożenia.

Trudności oraz nowości

CERT Polska napotyka znaczne trudności w docieraniu do właściwych administratorów systemów, co jest kluczowe dla skutecznego zarządzania cyberbezpieczeństwem. Głównym źródłem kontaktów jest baza RIPE, której dane często są nieaktualne lub mylące, szczególnie w przypadkach, gdy właściciel adresu IP nie jest jednocześnie administratorem urządzenia. Ponadto identyfikacja właściwego kontaktu z listy kilku adresów e-mail często komplikowana jest przez automatyczne systemy.

Kolejnym wyzwaniem jest przekonanie prywatnych właścicieli do podjęcia działań zabezpieczających, co nie zawsze jest możliwe ze względu na brak obowiązku lub umiejętności technicznych. W sytuacji, gdy zagrożenie może znacząco wpłynąć na bezpieczeństwo publiczne, takie jak w przypadku systemów sterowania oczyszczalniami ścieków, konieczna jest eskalacja incydentów, aby przyspieszyć ich rozwiązanie.

W odpowiedzi na te wyzwania CERT Polska planuje wdrożenie nowego systemu n6, który poszerzy możliwości monitoringu i raportowania poprzez integrację danych z zewnętrznych źródeł, takich jak Shadowserver. Nowy system umożliwi także bardziej efektywną dystrybucję powiadomień o potencjalnych podatnościach zarówno w technologiach operacyjnych (OT), jak i informacyjnych (IT), zwiększając tym samym skuteczność reakcji na cyberzagrożenia.

Konferencja Secure i międzynarodowe współprace

W minionym roku konferencja Secure zgromadziła ponad 300 uczestników dyskutujących o cyberbezpieczeństwie. CERT Polska aktywnie uczestniczyła w międzynarodowych ćwiczeniach i konkursach, wzmacniając współpracę w dziedzinie cyberbezpieczeństwa.

AUTOR
Klaudia Wojciechowska

Memorandum o współpracy w zakresie cyfryzacji między Polską a Ukrainą

Memorandum o współpracy w zakresie cyfryzacji podpisali przedstawiciele Polski i Ukrainy. Nasz kraj reprezentował Krzysztof Gawkowski, wicepremier i minister cyfryzacji. Ze strony ukraińskiej był to Mykhailo Fedorov, wicepremier ds. innowacji, rozwoju edukacji, nauki i technologii oraz minister transformacji cyfrowej Ukrainy.

Celem partnerstwa Polski i Ukrainy jest współpraca w dziedzinie technologii cyfrowych i innowacji, rozwój branży IT, sztucznej inteligencji, e-administracja. W ramach współpracy rozwijane będą także aplikacje mObywatel i Diia.

– Podpisaliśmy memorandum w celu rozszerzenia możliwości współpracy polsko-ukraińskiej. Osobiście widzę, a nasi ukraińscy przyjaciele potwierdzają to, że pomoc ze strony Polski ma realny wpływ na wiele aspektów funkcjonowania ludności ukraińskiej podczas wojny. Zrobimy wszystko, aby wzmocnić nasze wsparcie cyfrowe. Ukraina musi wygrać wojnę, a strategiczna współpraca polsko-ukraińska pomoże osiągnąć ten cel! – stwierdził Krzysztof Gawkowski, wicepremier i minister cyfryzacji.

Krzysztof Gawkowski w celu ustalenia współpracy odbył wizytę w Kijowie. Zapewnił, że polski rząd będzie nadal pokrywać opłaty za terminale. Pozwoli to na kontynuowanie korzystania z usług komunikacyjnych przez kluczowe obiekty infrastruktury bezpłatnie.

– Polska jest kluczowym partnerem w krajobrazie cyfrowym Ukrainy. W obliczu pełnowymiarowej inwazji Polska wykazała stałe wsparcie dla naszej infrastruktury cyfrowej na poziomie strategicznym. Polska stała się wiodącym dostawcą terminali Starlink dla Ukrainy, dzięki czemu ponad 20 000 terminali zwiększa

komunikację i dostęp do internetu dla Ukraińców. Jestem przekonany, że nasze partnerstwo będzie nadal przynosić liczne wspólne inicjatywy i znaczące projekty w przyszłości – powiedział Mykhailo Fedorov, wicepremier ds. innowacji, rozwoju edukacji, nauki i technologii oraz minister transformacji cyfrowej Ukrainy.

Wizyta była okazją do poruszenia tematu roli Polski jako głównego ośrodka analitycznego i koordynacyjnego Mechanizmu Tallińskiego (tzw. Back Office). Zapewnia to zaspokojenie średnio i długoterminowych potrzeb ukraińskiego systemu cyberbezpieczeństwa, wzmocnieniu odporności Ukrainy.

Zwieńczeniem wizyty było zwiedzanie Unit City, powstałego w 2020 r. centrum rozwoju nowych technologii oraz wspierania startupów, które nazywane jest ukraińską Doliną Krzemową. Odbyło się tam spotkanie z przedstawicielami Ukraińskiego Funduszu Startupów.

CELEM PARTNERSTWA POLSKI I UKRAINY JEST WSPÓŁPRACA W DZIEDZINIE TECHNOLOGII CYFROWYCH I INNOWACJI, ROZWÓJ BRANŻY IT, SZTUCZNEJ INTELIGENCJI, E-ADMINISTRACJA. W RAMACH WSPÓŁPRACY ROZWIJANE BĘDĄ TAKŻE APLIKACJE MOBYWATEL I DIIA

JAMBOX

TELEWIZJA ŚWIATŁOWODOWA

www.jambox.pl

tv smart

DEKODERY IPTV

Arris 4302 HD

Arris 5202 4K

CatchUp
7 DNI WSTECZ

StartOver
OGLĄDAJ OD POCZĄTKU

JAMBO Nagrywarka
NAGRYWAJ W CHMURZE

tv smart GO

NOWOŚĆ!

ZAMÓW TERAZ NA BEZPŁATNE TESTY
sgt.net.pl

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

TV Smart to także:

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

TELEFONIA KOMÓRKOWA

JAMBOX mobile

LTE 5G

VoLTE Wi-Fi Calling

Blisko **300** kanałów, w tym **185** w jakości HD i **5** UHD 4K

Atrakcyjna oferta pakietowa

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

- 16 lat na rynku IPTV, 570 partnerów ISP
- 160 tys. abonentów JAMBOX
- Nowoczesne autorskie oprogramowanie HD dekoderów
- Zaawansowany system zarządzania usługami
- Dystrybucja usługi w multicast i unicast
- Wsparcie marketingowo-sprzedażowe
- **JAMBOX go!** – oglądanie TV i zarządzanie usługami ze smartfona, komputera czy tabletu
- **JAMBOX mobile** – telefonia i mobilny Internet LTE i 5G, proste przenoszenie numerów, rozmowy z prędkością technologii LTE i zawsze pewny zasięg dzięki Wi-Fi Calling

SGT

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

sgt.net.pl/iptv-dla-isp

Zadzwoń lub wyślij email

32 428 8 428 handlowy@sgt.net.pl

AUTOR
Marcin Zemła

Macie to czarno na białym – dyrektywa NIS2 dotyczy MiŚOT-ów

Pojawiła się nowa wersja projektu ustawy o krajowym systemie cyberbezpieczeństwa, która wdraża dyrektywę NIS2. Zasady dotyczą wszystkich małych i średnich operatorów telekomunikacyjnych. Koniec dyskusji. Szach-mat. Tak jak mówiliśmy.

Jeszcze na naszym ostatnim spotkaniu w Janowie Podlaskim charyzmatyczni piewcy antysystemowi, o podejściu raczej spółdzielczym i anarchicznym niż przedsiębiorczym,

zakrzyczeli coś ważnego, co staraliśmy się Wam przekazać. Niektórzy z Was będą kluczowi niezależnie od wielkości (jeśli bawicie się DNS-ami), a niektórzy będą ważni. Nie zmienia to jednak faktu, że obowiązki wynikające z dyrektywy NIS2 będziecie musieli spełnić. Takie same w zakresie kontroli i zabezpieczeń systemu zarządzania biznesem.

Mówiłem też w Janowie Podlaskim, że stoicie przed życiową decyzją. Albo się dostosujecie i będziecie się rozwijać (jeśli chcecie robić dalej to, co robicie, patrząc, jak rośniecie i stosując się do zasad), albo będzie ciężko.

Patrząc kapitalistycznie, za pogląd na świat się płaci. To luksus. I będzie miał swoją wymierną cenę – w grzywnach. Chcesz być wyjątkowy i być trzmielem z NASA – doceniamy. Ale świat idzie w innym kierunku i płacisz za tę wyrwę w systemie 200 tys. PLN, bo to my odpowiadamy za bezpieczeństwo kraju. I przyjedziemy ponownie sprawdzić, czy czasem nie zmieniłeś zdania, bo jak nie, to weźmiemy 400 tys. PLN.

To konsekwencje, które staramy się Wam pokazać już od jakiegoś czasu. I to jest główne ryzyko zmian wprowadzanych z tytułu historii Sars czy wojny w Europie.

Będziecie dumni z tego, że jesteście antysystemowi? Poczekacie i zobaczycie? Nie dacie się przestraszyć?

PATRZĄC KAPITALISTYCZNIE, ZA POGLĄD NA ŚWIAT SIĘ PŁACI. TO LUKSUS. I BĘDZIE MIAŁ SWOJĄ WYMIERNĄ CENĘ – W GRZYWNACH

Polecam szybkie przekwalifikowanie na prowadzenie straganu z warzywami, bo ryzyko prowadzenia działalności telekomunikacyjnej w tym kraju bardzo wzrosło. Prowadzenie straganu oczywiście nie hańbi. Praca fajna, zdrowa, na świeżym powietrzu, nikt też nie będzie Wam mówił, jak macie prowadzić stragan, bo sami sobie sterem żeglarzem i okrętem.

Takie samo podejście do biznesu telekomunikacyjnego, w świetle najnowszego projektu ustawy o krajowym systemie cyberbezpieczeństwa, nie jest już adekwatne do zaistniałych zmian. Spółdzielca i przedsiębiorca to dwa różne punkty widzenia na rynek. Trzeba się przestawić z myśleniem.

Przez majówkę czytaliśmy ustawę o KSC. Niebawem odniosę się na łamach ISPortalu do kolejnych zawartych w niej zagadnień. Projekt MdS znał je wcześniej, bo czytaliśmy ze zrozumieniem unijną dyrektywę i na jej podstawie przygotowaliśmy adresowane do Was szkolenia. Od roku prosimy: szkolcie się! Reakcje? Nie, to wyciąganie kasy.

Pozwolę sobie – raz jeszcze – coś wyjaśnić waszym językiem. Projekt MdS został stworzony dla Was w celu zabezpieczenia rynku. Was. Masę czasu poświęcamy przy tym na rozwiązanie problemu z zasobami, tego ilu Was jest i problemów, o których wiemy od trzech lat i o których Wam jasno mówimy. Czarny scenariusz zbliża się przy tym dużymi krokami, jest coraz bardziej prawdopodobny i straszy teraz konkretnymi liczbami: 200 tysięcy, 400 tysięcy.

Wyliczanki zawarte w przepisach nie są może szczególnie ciekawe, ale warto je powtarzać, by dotarły do wszystkich, a jak już kiedyś dotarły, to żeby się utrwaliły. Artykuł 5 proponowanej przez rząd ustawy wskazuje podmioty kluczowe i ważne. Niektórzy z Was będą kluczowi niezależnie od wielkości (jeśli bawicie się DNS-ami), a nie niektórzy będą ważni. Nie zmienia to jednak faktu, że obowiązki wynikające z dyrektywy NIS2 będziecie musieli spełnić.

Dyrektywa obejmuje więc:

- podmioty średnie z załącznika I lub II, które są podmiotami ważnymi;
- przedsiębiorców telekomunikacyjnych będących mikro lub małymi przedsiębiorcami;
- średnie podmioty telekomunikacyjne (napisane jest tam: przedsiębiorca komunikacji elektronicznej i z definicji jesteście właśnie takimi podmiotami);
- dostawców usług DNS, niezależnie od wielkości (tutaj toczy się jeszcze walka, którą podjęła w Waszym imieniu Rada Bezpieczeństwa Biznesowego);
- dostawców usług zarządzania w zakresie cyberbezpieczeństwa;
- inne podmioty wskazane decyzją rządu na podstawie artykułu 7c.

Pozostałe punkty raczej Was nie dotyczą.

Projekt MdS natomiast będzie miał status podmiotu kluczowego i jest do tego przygotowywany od trzech lat. Dla Was.

Po wejściu w życie ustawy nie wystarczy już wzięcie na umowę kolegi Janka, który w garażu ogarnia Splunka i jest dobry (w Waszej opinii), bo jak go zakontraktujecie za miskę ryżu, to odpowiecie przy kontroli za robienie biznesu z podmiotem niespełniającym wymogów ustawy.

Co ciekawego się wydarzy?

Składacie wniosek, żeby się zarejestrować (do dwóch miesięcy od wejścia obowiązków) koniecznie z oświadczeniem: *Świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia wynikającej z art. 233 § 6 Kodeksu karnego oświadczam, że dane zawarte we wniosku są zgodne z prawdą*. Od tego momentu dotyczą Was obowiązki wynikające z artykułu 8 ustawy.

Jakie?

- prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem, czyli wdrożenie u Was całego systemu zarządzania i udowodnienie, że od momentu wejścia przepisów to działa – na razie jedna kartka papieru na miesiąc i ogrom pracy, żeby to się działo;
- wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, w szczególności, czyli udowodnienie, że wdrażacie działania korygujące wynikające z rejestru ryzyk i rejestru incydentów oraz przeglądacie własny system bezpieczeństwa, a wasza organizacja zakłada sobie za cel ich spełnienie;

SPÓŁDZIELCA I PRZEDSIĘBIORCA TO DWA RÓŻNE PUNKTY WIDZENIA NA RYNEK. TRZEBA SIĘ PRZESTAWIĆ Z MYŚLENIEM

- realizowanie polityk szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityk tematycznych: pełna, żyjąca polityka z wdrożonymi procedurami, opis działań, dowód, że się dzieją zgodnie z przyjętą normą;
- utrzymanie i bezpieczna eksploatacja systemu informacyjnego – dowody, logi w korelacji z dokumentacją, rejestrem ryzyk i incydentów;
- bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu oraz adekwatność zastosowanych środków dostępu do urządzeń (zgodnie z normą ma to wynikać z ryzyka i jego poziomu);
- bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy dostawcą sprzętu lub oprogramowania a podmiotem kluczowym, lub podmiotem ważnym, czyli badanie łańcucha dostaw, prowadzenie rejestru dostawców i analiza każdej dostawy;
- wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone

PROJEKT MDS NATOMIAST BĘDZIE MIAŁ STATUS PODMIOTU KLUCZOWEGO I JEST DO TEGO PRZYGOTOWYWANY OD TRZECH LAT. DLA WAS

świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, oraz planów awaryjnych umożliwiających odtworzenie systemu informacyjnego po katastrofie. To element normy ISO 22301. Trzeba zrobić analizy BIA i popatrzeć jakie zakłócenia mogą wyłożyć Wam firmę;

- system informacyjny wykorzystywany do świadczenia usługi systemem monitorowania w trybie ciągłym, czyli pole dla tych, którym cyberbezpieczeństwo kojarzy się z XDR, EDR, SIEM. Zastosowanie takich monitoringów musi być uzasadnione ryzykiem. Projekt MdS ma własne centrum monitorowania. Istnieje możliwość, by się do niego podłączyć. Oczywiście po wdrożeniu, bo musimy najpierw wiedzieć, co mamy podłączyć;
- polityki i procedury oceny skuteczności środków technicznych i organizacyjnych. System ma być skuteczny i to należy wykazać, a następnie móc później udowodnić, że polityki nasze są rzeczywiście skuteczne;
- edukacja z zakresu cyberbezpieczeństwa dla personelu podmiotu, w ramach której wytłumaczone zostaną podstawowe zasady cyberhigieny. MdS przygotował Wam Szkolenia, trąbimy o nich od roku. Zero odzewu z Waszej strony;
- polityki i procedury stosowania kryptografii, w tym szyfrowania (jeśli są konieczne);
- zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi. To załatwia Projekt MdS, będąc SOC. Nasz zespół Testów i Analiz gromadzi te informacje i rozdaje rekomendacje;
- zarządzanie incydentami w zakresie informacji o ich wystąpieniu, minimalizacji skutków, wdrożenia działań korygujących w oparciu o ryzyko;
- stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi;
- stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym;
- regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji;
- ochrona przed nieuprawnioną modyfikacją w systemie informacyjnym;
- niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub cyberzagrożeń;
- stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa, uwzględniających uwierzytelnianie wieloskładnikowe.

Wymagania, o których mowa uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301. Oczywiście możecie się certyfikować (tak jak dla Was zrobił to Projekt MdS), co nie zwolni Was z kontroli, ale może łagodniej ją przejdziecie.

Dużo? Owszem. A to nie koniec.

Co jeszcze musicie?

Macie prowadzić dokumentację, która jest opisana szczegółowo w artykule 10 projektu. Projekt MdS ma to także w swojej ofercie. Jeżeli zawierasz z nami umowę, dostajecie portal (jeśli nie masz własnego) i pełnomocnika, który za to odpowiada i chroni Was też w trakcie kontroli.

Macie zgłaszać incydenty i komunikować się z CSIRTEM (zapewne przez system S46).

Macie informować użytkowników o zagrożeniach. Trzeba wypracować mechanizmy. Projekt MdS już to robi.

Macie co dwa lata przeprowadzać na własny koszt audyt bezpieczeństwa. Jeśli Projekt MdS będzie Was obsługiwał i chronił, nie będzie mógł Was audytować, ale spokojnie – mamy do tego firmy zewnętrzne. Jesteśmy przygotowani. A Wy?

Skontaktujcie się z MdS.

Projekt MdS wdraża już wymagania dyrektyw NIS 2 u operatorów, a pełnego wdrożenia tych przepisów nie da się dokonać w kilka dni ani tygodni. Chcemy, abyście nadal mogli skupiać się na działalności telekomunikacyjnej

NIE BĘDZIE NAS STAĆ NA ZATRUDNIANIE KOLEJNYCH SPECJALISTÓW I OBSŁUGI WSZYSTKICH MAŁYCH I ŚREDNICH OPERATORÓW PO CENACH, KTÓRE SĄ PONIŻEJ RYNKOWYCH

w tych naprawdę trudnych warunkach, z którymi NATO oraz Unia Europejska radzą sobie dziś tak, jak potrafią.

Jeżeli uważacie, a usłyszałem to w Janowie Podlaskim, że ściągamy z Was kasę, powiem to jasno: przestanie być śmiesznie, jak nam się skończą zasoby. Wtedy to, w trosce o tych, którzy wcześniej nam zaufali, powiemy reszcie dosyć. Nie będzie nas stać na zatrudnianie kolejnych specjalistów i obsługi wszystkich małych i średnich operatorów po cenach, które są poniżej rynkowych. Nasze ceny są zaledwie SKŁADKĄ, drodzy spółdzielcy.

Z Projektem MiŚOT dla Security można skontaktować się, pisząc na e-mail: biuro@projektmds.pl lub wypełniając formularz kontaktowy na stronie: Kontakt – Projekt MdS.

AUTOR
Michał Koch

Bezpieczne finanse w cyfrowym świecie

Ponad połowa Polaków ufa instytucjom finansowym w kwestii cyberbezpieczeństwa. Badanie przeprowadzone przez Biostat wskazuje, że 53,6 proc. respondentów jest przekonanych, że ich środki finansowe są odpowiednio chronione. Czy to jednak dobrze?

Marcin Zemła, specjalista ds. bezpieczeństwa Grupy MiŚOT, zapewne odpowiedziałby, że nie. Potrafię sobie wyobrazić, że w tym momencie zaczynałby już wykład o tym, że nieustanna czujność to prawdziwy klucz do bezpieczeństwa. Gdyby Marcin dowiedział się, że aż 30,4 proc. ankietowanych nie jest w stanie podać jednoznacznej odpowiedzi na pytanie, zapewne byłby jeszcze bardziej przerażony.

Bać się czy nie?

Co ciekawe, największe przekonanie co do bezpieczeństwa środków finansowych online wykazały osoby w wieku od 18 do 29 lat. Osoby powyżej 50. roku życia najczęściej odpowiadały, że nie wiedzą. Różnica w podejściu może wynikać z różnych doświadczeń oraz stopnia zaawansowania technologicznego w poszczególnych grupach wiekowych.

W obecnym środowisku gospodarczym, w którym technologie cyfrowe odgrywają kluczową rolę w codziennych transakcjach, budowanie zaufania klientów poprzez zapewnienie im bezpieczeństwa staje się priorytetem dla każdej instytucji finansowej. Zaufanie do bankowości jest nawet w Polsce uznawane za jeden z celów nadzoru nad rynkiem finansowym. Również prestiż i wizerunek to coś, na czego stratę instytucje finansowe nie mogą sobie pozwolić.

Niewiedza czy bezrefleksyjne zaufanie? To odwieczny konflikt, który być może nie ma łatwego rozwiązania. Łatwo odpowiedzieć, że najlepszym wyjściem jest złoty środek, czyli kontrola i ograniczone zaufanie. Jednakże często korzystając np. z bankowości internetowej, jesteśmy skazani na rozwiązania, które zna przede wszystkim bank (oby nie znali ich cyberprzestępcy!).

JEDNAKŻE CZĘSTO KORZYSTAJĄC NP. Z BANKOWOŚCI INTERNETOWEJ, JESTEŚMY SKAZANI NA ROZWIĄZANIA, KTÓRE ZNA PRZEDE WSZYSTKIM BANK (OBY NIE ZNALI ICH CYBERPRZESTĘPCY!)

Bezpieczeństwo finansowe to nie tylko kwestia technologii, ale także naszej własnej świadomości i odpowiedzialności.

Ta podstępna biometria

Bank BNP Paribas chwali się, że uruchomił opcję ochrony behawioralnej. Aplikacja mobilna ma rozpoznać, gdy zacznie z niej korzystać ktoś inny niż właściciel konta.

– Wykorzystanie ochrony behawioralnej to przyszłość cyberbezpieczeństwa i cieszę się, że jesteśmy wśród pierwszych instytucji, które wdrażają takie rozwiązania – mówi Krzysztof Słotwiński, dyrektor zarządzający pionu bezpieczeństwa w banku.

Na czym polega ochrona behawioralna? Dzięki machine learning aplikacja uczy się sposobu, w jaki na co dzień obsługuje ją właściciel (dotyczy to zarówno sposobu klikania, jak i nawet różnic w trzymaniu telefonu) i alarmuje bank, gdy dane te się nie zgadzają. W teorii ma to oznaczać, że dostęp do konta uzyskała osoba trzecia, a bank bezzwłocznie informuje o tym posiadacza rachunku bankowego.

Trzeba zaznaczyć, że zastosowany system nie zapisuje tego, co użytkownik wpisuje na klawiaturze. Badane jest wyłącznie to, jak aplikacją posługuje się użytkownik. Tu jednak mogą pojawić się wątpliwości, bo przecież byliśmy już świadkami sytuacji, gdy dopiero po jakimś czasie wychodziło na jaw, że dane wrażliwe były jednak agregowane. Co może również prowadzić do złamania zasad cyberbezpieczeństwa.

Zatem czy pieniądze trzymać jednak w domowym sejfie lub – o zgrozo! – w skarpecie w szufladzie? Nie, to nie jest dobre rozwiązanie. Bądźmy świadomi rozwiązań bezpieczeństwa, które oferuje nasz bank i – a być może przede wszystkim – bądźmy czujni i rozważni. Począwszy od banałów, czyli nieinstalowania oprogramowania niewiadomego pochodzenia na komputerze i smartfonie, po stosowanie haseł rotacyjnych i kluczy U2F aż po analitykę: regularne monitorowanie swoich rachunków bankowych i transakcji, aby szybko wykryć ewentualne nieprawidłowości.

TRENDY

AUTOR
Klaudia Wojciechowska

Naukowcy pracują nad kwantowym internetem

Na razie nie ma jeszcze komputerów kwantowych i w najbliższym czasie raczej się nie pojawią. Nie powstrzymuje to naukowców przed pracami nad kwantowym internetem. Czy rozwiązaniem powinny zainteresować się również rządy?

Kwantowy internet ma być sposobem na łączenie ze sobą komputerów kwantowych. Pewnego dnia pozwoli to ludziom wykonywać obliczenia i wymieniać dane danych między odległymi urządzeniami. Wszystko to na razie

w obszarze teorii, bo nie ma kwantowych komputerów. Ale naukowcy pracują nad kwantowym internetem.

Uważają oni, że w przyszłości kwantowe sieci komunikacyjne przysłużą się rozwiązywaniu złożonych problemów w dziedzinie finansów, medycyny i badań naukowych, którymi nie poradzą sobie pojedyncze komputery kwantowe. Pozwoli to także na prawie niemożliwe do złamania szyfrowanie, co podniesie poziom zabezpieczeń wiadomości przesyłanych w systemach kwantowych.

Internet kwantowy to ogromne wyzwanie

Podobnie jak w przypadku komputerów kwantowych, tak samo w przypadku kwantowego internetu wyzwaniem jest podporządkowanie działania całości mechanice kwantowej. Dotychczas nikt nie stworzył stabilnej sieci kwantowej na dużą skalę, co wynika z tego, że kluczowa technologia podtrzymywania połączenia – tzw. wzmacniacz kwantowy na razie nie istnieje.

W zwykłych sieciach takie wzmacniacze używane są do wzmacniania sygnałów na duże odległości. Takie same rozwiązania w systemach kwantowych są na razie nieosiągalne. Dlatego naukowców fascynuje to zagadnienie i starają się znaleźć sposoby na rozwiązanie problemu.

Budują oni sieci kwantowe jako platformy testowe do przesyłania informacji na odległości dziesiątek kilometrów. Zajmują się tym grupy z Uniwersytetu Harvarda

i Chińskiego Uniwersytetu Nauki i Technologii. Ich eksperymenty w dziedzinie kwantowej czasopismo „Nature" nazwało „najbardziej zaawansowanymi jak dotąd demonstracjami technologii potrzebnej do zbudowania kwantowego Internetu".

– Z centrum miasta obejmujesz zasięgiem wiele osób i wiele firm, co oznacza, że możesz już myśleć o praktycznych sieciach kwantowych, które nie potrzebują repeatera [red. wzmacniacza kwantowego]. Być może nie będzie to działać między miastami, ale w regionach metropolitalnych można zacząć wdrażać tę technologię, a to samo w sobie dla instytucji finansowych i wielu zastosowań byłoby fantastyczne – wyjaśnia David Awschalom, kierujący Chicago Quantum Exchange.

Jak rządy powinny angażować się w sieci kwantowe?

W Stanach Zjednoczonych rząd finansował naukę leżącą u podstaw mechaniki kwantowej przez dziesiątki lat. Teraz to źródła finansowania osłabło. Dzieje się to w momencie, gdy rozwiązania kwantowe potrzebują pomocy w przejściu od odkryć naukowych – poziomu teoretycznego – do opracowywania aplikacji biznesowych – poziomu praktycznego. To wymaga jeszcze większych nakładów finansowych. Jednocześnie nie ma szans, by pozyskać je z sektora prywatnego.

Jane Bambauer, profesor prawa z Uniwersytetu Florydy, uznaje, że sektor prywatny nie osiągnie zysków z technologii kwantowej w najbliższym czasie. Dzieje się tak pomimo wzrostu liczby startupów zajmujących się technologiami kwantowymi czy większej liczby firm tym zainteresowanych. Praktyczne zastosowanie technologii jest odległe w czasie, a jako takie nie stanowi pewnika dla inwestorów.

Naukowcy i firmy zajmujące się technologiami kwantowymi są zależne od finansowania federalnego. Ponadto to rząd ma wpływ na rozwiązania związane z rozwojem siły roboczej i ustanawiania standardów, które wiążą się z technologiami kwantowymi.

W STANACH ZJEDNOCZONYCH RZĄD FINANSOWAŁ NAUKĘ LEŻĄCĄ U PODSTAW MECHANIKI KWANTOWEJ PRZEZ DZIESIĄTKI LAT. TERAZ TO ŹRÓDŁA FINANSOWANIA OSŁABŁO

Przewodniczący komisji ds. nauki w Izbie Reprezentantów USA Frank Lucas zwraca uwagę na ten problem. Zauważa, że „innowacje rozwijają się dzięki stabilnemu, przewidywalnemu finansowaniu". Brak pieniędzy na badania nad technologiami kwantowymi powstrzyma ich rozwój na długi czas. Dlatego Lucas i Zoe Lofgren, kolejna członkini komisji,naciskają na określenie priorytetów naukowych, biznesowych i bezpieczeństwa USA dla mechaniki kwantowej. Miałoby to zapewnić stabilność ich finansowania na najbliższe pięć lat.

FELIETON

AUTOR
Michał Koch

Ktoś jeszcze wierzy w metawersum?

Praca zdalna, wirtualne eventy oraz cyfrowa rzeczywistość pod postacią metawersum. W czasach pandemii koronawirusa – minęły już cztery lata od wprowadzenia lockdownu! – wszystkim wydawało się, że świat już na stałe pozostanie cyfrowy. Myliliśmy się.

Koncepcja metawersum jako wirtualnej przestrzeni, w której ludzie żyją i doświadczają quasi-realnych zdarzeń, wprowadzona została po raz pierwszy w powieści sf Neala Stephensona pt. „Snow Crash" w 1992 roku. Od tamtego czasu raz po raz pojawia się na kartach powieści fantastycznych.

Wierzymy, że metawersum to przyszłość komunikacji. Taki slogan widnieje na stronie Mety (spółki zarządzającej Facebookiem i Metaverse). Nie pamiętam, kiedy bardziej się z czymś nie zgadzałem.

Większość cyfrowych aktywności miała przynajmniej jakiś sens. Ba, home office pozwalał funkcjonować zarówno firmom, jak i utrzymać źródło dochodów dla wielu ludzi. Metawersum jednak zawsze było tylko dziecinnym gimmickiem. Czy ktoś uwierzył, że ludzie, istoty w ogromnej mierze społeczne, będą w stanie prawie całkowicie przenieść wszystkie aktywności do cyberprzestrzeni? Dziś wierzy w to już chyba tylko, jeśli w ogóle, Mark Zuckerberg.

Zresztą Meta wydała już ponad 46 mld USD na rozwój pomysłu. Zysków jednak nie widać.

Amerykańska sieć supermarketów Walmart otworzyła i zamknęła własną markę metawersum już po sześciu miesiącach, w Google zakończyli prace nad wirtualną przestrzenią w czerwcu ubiegłego roku, a zarządcy Disneya zatwierdzili rozwiązanie całego zespołu, który pracował nad tym konceptem.

W obliczu tych zdarzeń wydaje się, że Orange Polska spóźnił się na przyjęcie.

Firma zaprezentowała Orange Business Metaverse, czyli narzędzie, które w teorii ma prezentować możliwości smart city i sieci kampusowych 5G ich klientom biznesowym. W wirtualnym świecie mają odbywać się prezentacje i szkolenia, które dzięki temu uzyskają bardziej atrakcyjną formę.

Związek Cyfrowa Polska apeluje natomiast do rządu o opracowanie narodowej strategii metawersum. Miałoby to pozwolić firmom w końcu zarabiać na wirtualnym świecie. Michał Kanownik, prezes związku, jest zdania, że metawersum potrzebuje szczegółowych regulacji prawnych. Pozwoliłoby to rozwinąć możliwości szkolenia m.in. pracowników służby zdrowia oraz nauczycieli za pomocą immersyjnych metod dydaktycznych.

W oświadczeniu ZCP czytamy:

Takie technologie, jak AI czy metawersum, rewolucjonizują sposób pracy, nauki i komunikacji. O ile Bruksela zajęła się AI, a rząd prowadzi prekonsultacje dotyczące wdrożenia unijnego AI Act, o tyle w przypadku VR/AR brakuje podobnego impulsu. W resorcie cyfryzacji zapewniają, iż są świadomi znaczenia metawersum.

Sprawdza się stara prawda, że jeśli nie wiadomo, o co chodzi, to chodzi o pieniądze. Podnoszą się głosy, że rząd powinien wprowadzić ulgę B+R (Business+Research) związaną z produktami AI i metawersum.

Raport The Potential Global Economic Impact of the Metaverse przewiduje, że metawersum ma wkrótce odpowiadać za 2,8 proc. globalnego PKB, a wartość tylko polskiego rynku wirtualnej rzeczywistości ma wynieść 10 mld USD do 2035 roku. Cóż, rzeczywistość – tym razem ta realna – zweryfikuje te przewidywania.

CZY KTOŚ UWIERZYŁ, ŻE LUDZIE, ISTOTY W OGROMNEJ MIERZE SPOŁECZNE, BĘDĄ W STANIE PRAWIE CAŁKOWICIE PRZENIEŚĆ WSZYSTKIE AKTYWNOŚCI DO CYBERPRZESTRZENI?

W wirtualnym świecie mają odbywać się prezentacje i szkolenia, które dzięki temu uzyskają bardziej atrakcyjną formę.

AUTOR
Krzysztof Kołodziej

Wirtualizacja Proxmox – kopia zapasowa

Wstęp

Backup maszyn wirtualnych (VM) jest kluczowym elementem strategii zarządzania danymi w nowoczesnych centrach danych. Pozwala na zapewnienie ciągłości działania, ochrony danych oraz szybkie przywrócenie funkcjonalności systemów w przypadku awarii. Oto kilka kluczowych aspektów dotyczących backupu maszyn wirtualnych:

1. Rodzaje Backupów Maszyn Wirtualnych

Pełny Backup: Kopiuje całą maszynę wirtualną, włączając w to system operacyjny, aplikacje, dane oraz ustawienia konfiguracyjne. Jest najbardziej czasochłonny, ale daje najbardziej kompletną kopię zapasową.

Backup Różnicowy: Kopiuje tylko te dane, które zmieniły się od ostatniego pełnego backupu. Jest szybszy i wymaga mniej miejsca na przechowywanie niż pełny backup.

Backup Przyrostowy: Kopiuje tylko te dane, które zmieniły się od ostatniego backupu (pełnego lub różnicowego). Jest najbardziej efektywny pod względem czasu i przestrzeni, ale przywracanie danych może być bardziej skomplikowane.

2. Metody Backupowania

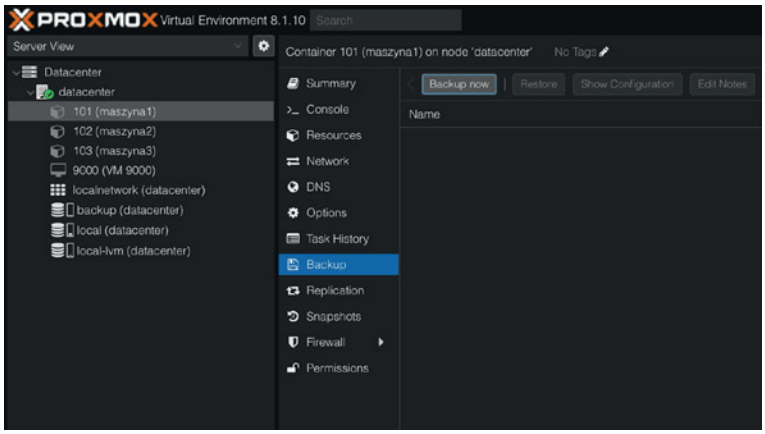
Agent-based Backup: Wymaga zainstalowania agenta backupowego na każdej maszynie wirtualnej. Daje precyzyjną kontrolę nad tym, co jest backupowane, ale może być trudne do zarządzania w dużych środowiskach.

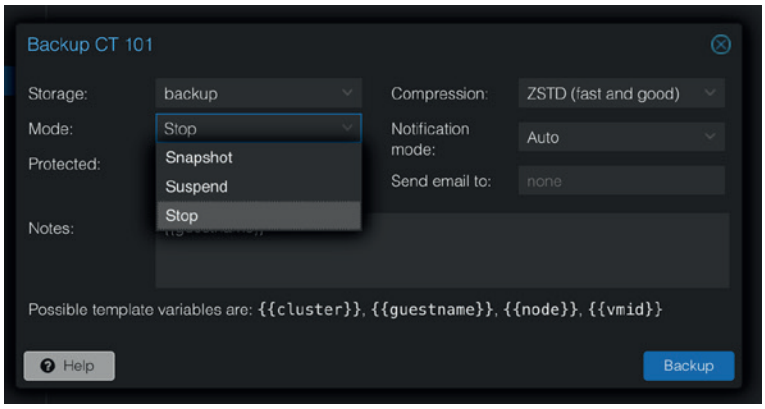
Agentless Backup: Backup wykonywany na poziomie hypervisora (Proxmox). Jest łatwiejszy w zarządzaniu i mniej obciąża zasoby systemowe.

Ręczny
EXPORT/IMPORT maszyny

Wykonanie kopii

Najprostsza metoda wykonania kopii maszyny/kontenera to skorzystanie z narządza **vzdump**. Program dostępny jest z linii komend. Alternatywnie można wykonać backup z poziomu GUI.





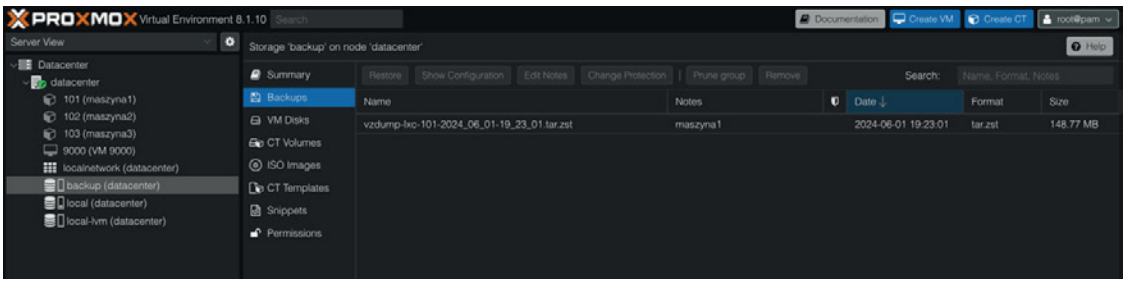
Dostępne są trzy tryby wykonania backupu:

Snapshot backup to mechanizm tworzenia kopii zapasowej na podstawie snapshotu, stanu maszyny wirtualnej lub kontenera. Snapshoty przechowują stan maszyny w danym momencie, co pozwala na szybkie i spójne tworzenie kopii zapasowych bez konieczności przerywania działania maszyny.

Suspend w tym trybie, maszyna wirtualna lub kontener są zawieszane a następnie tworzona jest ich kopia. Po zakończeniu backupu, praca maszyny jest wznawiana.

Stop w tym trybie, maszyna wirtualna lub kontener są najpierw zatrzymywane, a następnie tworzona jest ich pełna kopia. Po zakończeniu backupu, maszyna jest ponownie uruchamiana. Pomimo, iż ta metoda wymaga wykonania najdłuższej przerwy w działaniu maszyny, uznawana jest za najbardziej bezpieczną, wiarygodną.

Weryfikacja poprawności wykonania backupu:

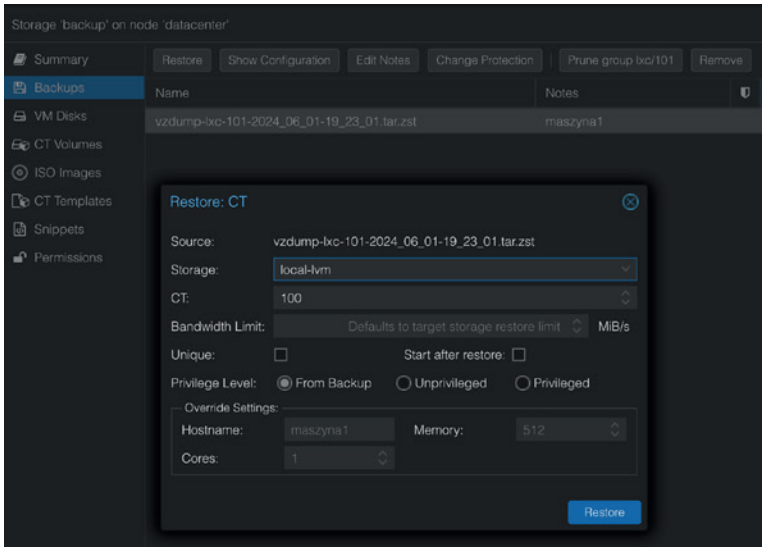


Powinniśmy zobaczyć nowoutworzony plik z rozszerzeniem tar.zst

Tak wykonany backup/export maszyny/kontenera można przesłać za pomocą komendy scp na dowolny serwer linux lub do innej instancji Proxmox.

Przywrócenie maszyny/kontenera

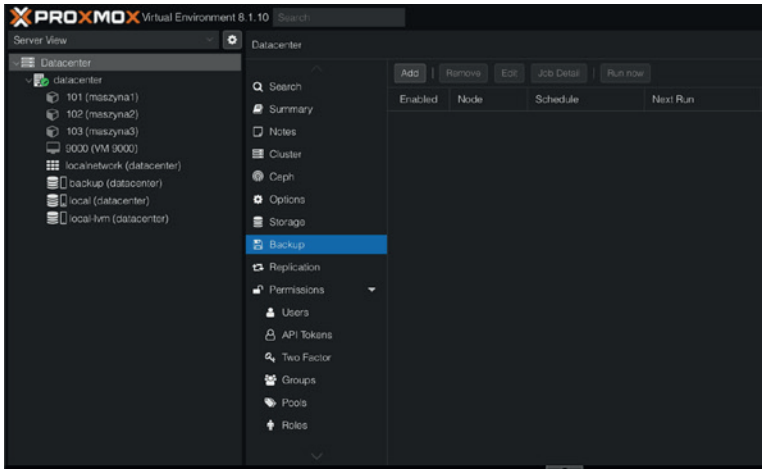
Podobnie jak wykonanie kopii, przywrócenie można wykonać z GUI lub linii komend (qmrestore, pct restore).

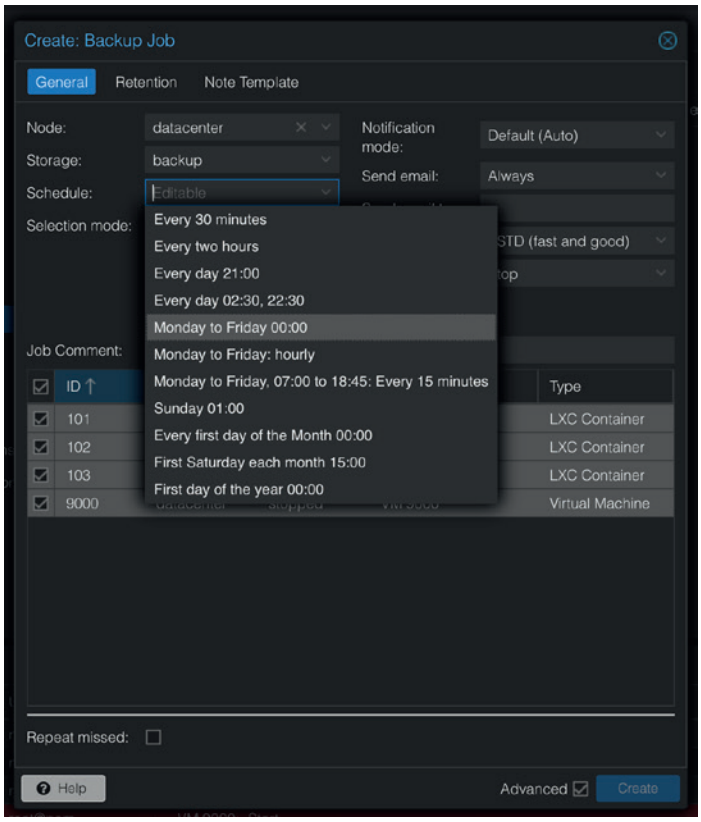


Podczas przywracania wskazujemy storage, na jakim umieszczona zostanie maszyny/kontener oraz id maszyny.

Harmonogram wykonywania BACKUP'u

Bardziej zaawansowaną opcją wykonywania kopii bezpieczeństwa, od ręcznego wykonywania jest stworzenie harmonogramu kopii zapasowej. Konfiguracja zadania dostępna jest na zakładce **Datacenter/Backup**.





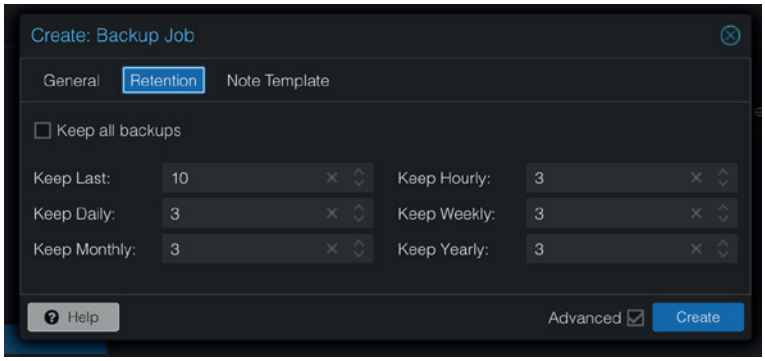
Storage należy wskazać magazyn danych, gdzie odkładane będą backup'y

Schedule to zaawansowana opcja pozwalająca na określenie kiedy, w jakich godzinach, w jakie dni tygodnia wykonywane będzie zadanie kopii zapasowej, poza predefiniowanymi zakresami można tutaj wprowadzić wartości customowe

Send email włączenie powiadomienia o wykonanym/niewykonanym zadaniu

Oczywiście należy też wybrać jakie maszyny/kontenery będą objęte harmonogramem

Ważnym elementem jest też wskazanie jak długo będą przechowywane kopie. Do tego służy zakładka **Retention**.



Dzięki tej opcji unikniemy sytuacji, gdzie kopie bezpieczeństwa w sposób niekontrolowany zajmą całą przestrzeń dyskową.

PBS INTEGRUJE SIĘ Z PROXMOX VE I OFERUJE ZAAWANSOWANE FUNKCJE ZARZĄDZANIA KOPIAMI ZAPASOWYMI MASZYN WIRTUALNYCH (VM), KONTENERÓW ORAZ FIZYCZNYCH HOSTÓW

Proxmox Backup Server

Proxmox Backup Server (PBS) to dedykowane rozwiązanie do tworzenia kopii zapasowych, które zostało zaprojektowane z myślą o wysokiej wydajności, elastyczności i bezpieczeństwie. PBS integruje się z Proxmox VE i oferuje zaawansowane funkcje zarządzania kopiami zapasowymi maszyn wirtualnych (VM), kontenerów oraz fizycznych hostów. Jest to najbardziej zaawansowane i wszechstronne rozwiązanie z dotychczas omawianych. PBS instaluje się z obrazu ISO i może zostać wdrożone jako maszyna wirtualna (np na serwerze typu NAS: Synology/QNAP). Poniżej znajduje się szczegółowy opis funkcjonalności Proxmox Backup Server.

Kluczowe Funkcje Proxmox Backup Server

1. Deduplikacja i Kompresja

- **Opis**: PBS wykorzystuje deduplikację na poziomie bloków, co pozwala na znaczne zmniejszenie ilości przechowywanych danych. Dzięki deduplikacji tylko unikalne bloki danych są przechowywane, co zwiększa efektywność przestrzeni dyskowej.
- **Kompresja**: Dodatkowo, dane mogą być kompresowane (np. przy użyciu algorytmów ZSTD), co jeszcze bardziej zmniejsza rozmiar kopii zapasowych.

2. Szyfrowanie

- **Opis**: PBS wspiera szyfrowanie AES-256 na poziomie klienta, co zapewnia, że dane są szyfrowane przed przesłaniem do serwera backupowego. Dzięki temu dane są chronione zarówno podczas przesyłania, jak i w stanie spoczynku.
- **Bezpieczeństwo kluczy**: Klucze szyfrowania są zarządzane przez użytkownika, co zwiększa poziom bezpieczeństwa.

3. Inkrementalne Kopie Zapasowe

- **Opis**: PBS wspiera tworzenie przyrostowych kopii zapasowych, co oznacza, że po pierwszym pełnym backupie, kolejne kopie zapasowe zawierają tylko zmiany dokonane od ostatniego backupu.
- **Zalety**: Znacznie zmniejsza to czas tworzenia kopii zapasowych oraz ilość przesyłanych i przechowywanych danych.

4. Centralne Zarządzanie

- **Interfejs Webowy**: PBS oferuje intuicyjny interfejs webowy do zarządzania kopiami zapasowymi, co umożliwia łatwe tworzenie, harmonogramowanie i monitorowanie zadań backupowych.

- **Integracja z Proxmox VE**: PBS integruje się bezproblemowo z Proxmox VE, umożliwiając centralne zarządzanie kopiami zapasowymi dla wielu klastrów.

5. Wielowarstwowe Przechowywanie

- **Opis**: PBS umożliwia konfigurację różnych poziomów przechowywania kopii zapasowych (np. lokalne dyski, sieciowe systemy plików, zewnętrzne magazyny danych), co zwiększa elastyczność i możliwości zarządzania przestrzenią dyskową.

6. Planowanie i Automatyzacja

- **Harmonogramowanie zadań**: Użytkownicy mogą tworzyć zaawansowane harmonogramy backupów przy użyciu formatu CRON, co pozwala na automatyzację procesu tworzenia kopii zapasowych.
- **Polityki przechowywania**: PBS wspiera zaawansowane polityki przechowywania, które pozwalają na automatyczne zarządzanie starymi kopiami zapasowymi.

7. Replikacja Zdalna

- **Opis**: PBS umożliwia replikację kopii zapasowych do zdalnych lokalizacji, co zapewnia dodatkowy poziom ochrony danych w przypadku awarii lokalnych systemów.

Proces Tworzenia Kopii Zapasowej i Przywracania

Tworzenie Kopii Zapasowej

1. **Konfiguracja Zadań Backupowych**: Użytkownik konfiguruje zadania backupowe poprzez interfejs webowy PBS, wybierając maszyny wirtualne, kontenery lub fizyczne hosty, które mają być objęte kopią zapasową.
2. **Automatyzacja**: Zadania mogą być harmonogramowane do automatycznego uruchamiania w określonych odstępach czasu.

BACKUP MASZYN WIRTUALNYCH (VM) JEST KLUCZOWYM ELEMENTEM STRATEGII ZARZĄDZANIA

3. **Deduplikacja i Kompresja**: Podczas tworzenia kopii zapasowej PBS deduplikuje i kompresuje dane w czasie rzeczywistym.

Przywracanie Danych

1. **Wybór Punktu Przywracania**: Użytkownik wybiera odpowiedni punkt przywracania (snapshot) z listy dostępnych kopii zapasowych.
2. **Przywracanie**: PBS oferuje szybkie i elastyczne opcje przywracania, umożliwiając przywracanie całych maszyn wirtualnych, pojedynczych kontenerów lub określonych plików i folderów.
3. **Spójność Danych**: Dzięki wsparciu dla snapshotów i przyrostowych backupów, PBS zapewnia spójność danych podczas procesu przywracania.

Korzyści z Używania Proxmox Backup Server

- **Efektywność Przechowywania**: Dzięki deduplikacji i kompresji, PBS znacznie zmniejsza ilość wymaganej przestrzeni dyskowej.
- **Bezpieczeństwo**: Szyfrowanie danych zapewnia ochronę przed nieautoryzowanym dostępem.

PBS INSTALUJE SIĘ Z OBRAZU ISO I MOŻE ZOSTAĆ WDROŻONE JAKO MASZYNA WIRTUALNA (NP NA SERWERZE TYPU NAS: SYNOLOGY/QNAP)

- **Automatyzacja**: Harmonogramowanie i polityki przechowywania umożliwiają automatyzację procesu tworzenia kopii zapasowych, co zmniejsza ryzyko błędów ludzkich.
- **Elastyczność**: Obsługa różnych typów magazynów danych oraz replikacja zdalna zapewniają elastyczne opcje przechowywania i ochrony danych.

Podsumowanie

Planując rozwiązanie backupowe warto zwrócić uwagę na następujące zagadnienia:

Regularne Testy Przywracania: Regularne testowanie procedur przywracania, aby upewnić się, że backupy są użyteczne i dane można szybko odzyskać.

Planowanie Harmonogramów Backupów: Ustalanie odpowiednich harmonogramów backupów, aby minimalizować wpływ na wydajność systemów produkcyjnych.

Kopia Zapasowa Poza Miejsce Pracy/ Zdalna Lokalizacja: Przechowywanie kopii zapasowych w oddzielnej lokalizacji, aby chronić dane przed lokalnymi awariami, takimi jak pożar czy powódź.

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