

# CYFROWY SEKTOR PUBLICZNY

Praktyczne rozwiązania i kierunki rozwoju



**ODPORNOŚĆ I NIEZALEŻNOŚĆ.  
SUWERENNOŚĆ TECHNOLOGICZNA  
ADMINISTRACJI PUBLICZNEJ**

Temat wydania

**OD INTRANETU DO ODPOWIEDZIALNE-  
GO ZARZĄDZANIA. JAK INTEGRACJA  
Z CEPIK OGRANICZYŁA RYZYKO  
I USPRAWNIŁA ORGANIZACJĘ PRACY?**

Studium przypadku

**SOCJOTECHNIKA. JAK DZIAŁAJĄ  
CYBEROSZUŚCI I JAK CHRONIĆ SIĘ  
PRZED ZAGROŻENIEM Z ICH STRONY?**

Wywiad numeru

**MULTIPORTAL ZMIENIA LOGIKĘ  
CYFRYZACJI JEDNOSTEK  
SAMORZĄDU TERYTORIALNEGO**

Krótki komentarz

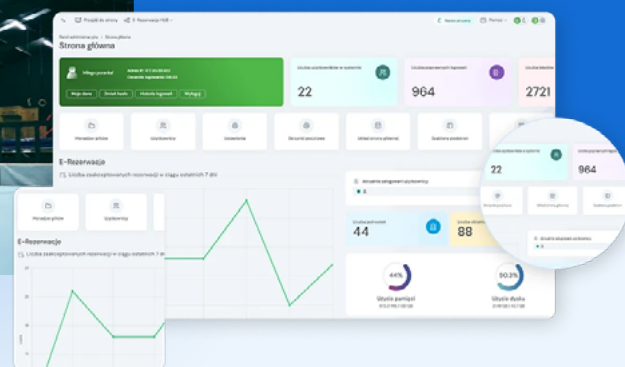
# Poznaj skalę korzyści cyfrowej rezerwacji obiektów sportowych

Cyfrowa rezerwacja to dla mieszkańców wygodny dostęp do rezerwacji online, dla właścicieli i administratorów łatwiejsza obsługa wynajmu, a dla JST dostęp do danych o wykorzystaniu infrastruktury sportowej.

**Sprawdź, jak zmienić obiekty sportowo-rekreacyjne z pozycji kosztowej w lepiej wykorzystywany zasób JST.**



Zeskanuj kod  
lub wpisz:  
<https://opteam.pl/e-sport>



01.

## Rentowność

Większe zainteresowanie wynajmem przekłada się na realne zyski dla właścicieli obiektów, szkół i JST.

02.

## Operacyjność

Łatwy dostęp do informacji o dostępności obiektu, rezerwacja i płatność online ułatwiają zarządzanie wynajmem.

03.

## Wizerunek

Cyfryzacja e-usług to pozytywny wizerunek władz powiatu, miasta oraz gminy w społeczności lokalnej.

## Spis treści

### Studium przypadku

- 02** Od Intranetu do odpowiedzialnego zarządzania. Jak integracja z CEPIK ograniczyła ryzyko i usprawniła organizację pracy?

### Temat wydania

- 06** Odporność i niezależność. Suwerenność technologiczna administracji publicznej

### Artykuły praktyczne

- 10** Samoobsługa pracownicza. Cyfrowe rozwiązanie, które usprawnia kadry w urzędzie.
- 12** Kultura organizacyjna w jednostkach samorządu terytorialnego
- 14** Zastosowania sztucznej inteligencji w jednostkach samorządu terytorialnego

### Wywiad numeru

- 16** Socjotechnika. Jak działają cyberoszuści i jak chronić się przed zagrożeniem z ich strony?

### Opinie ekspertów

- 22** Jak wiedza i doświadczenie administratorów IT w urzędach wpływa na bezpieczeństwo całej jednostki i realizację wymagań Krajowego Systemu Cyberbezpieczeństwa? W jaki sposób skutecznie rozwijać ich kompetencje?
- 22** Jakie są najczęstsze wyzwania przy wdrażaniu samoobsługi pracowniczej w sektorze publicznym w związku ze złożonością obowiązujących procedur?
- 23** Na jakich obszarach powinny skupiać się JST w pierwszej kolejności, aby uzyskać największy efekt w zakresie bezpieczeństwa przy ograniczonych budżetach?

### Krótki komentarz

- 24** Multiportal zmienia logikę cyfryzacji jednostek samorządu terytorialnego

### Redakcja

Krzysztof Pliś  
Bogumiła Szewdo

Magdalena Tobiasz  
Aleksandra Stachowicz

2026 OPTeam SA  
Wszelkie prawa zastrzeżone.

**Zdjęcia:**  
[www.magnific.com/pl/app](http://www.magnific.com/pl/app)

[www.pexels.com/pl-pl/](http://www.pexels.com/pl-pl/)  
[www.shutterstock.com](http://www.shutterstock.com)

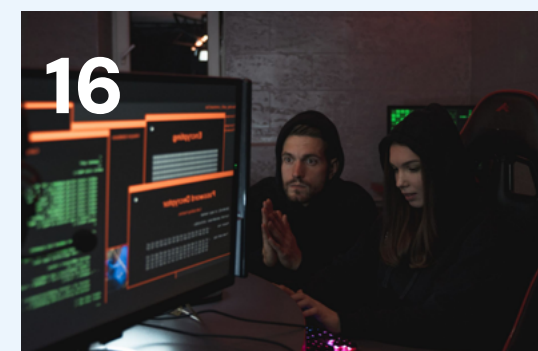
Treści prezentowane przez autorów w materiałach nie są wiążące i stanowią wyłącznie subiektywną opinię, będącą wynikiem ich spostrzeżeń i doświadczeń. Redakcja i wydawca nie odpowiadają za treść reklamodawców. Niektóre obrazy wygenerowano z pomocą AI.



Studium przypadku

### Od Intranetu do odpowiedzialnego zarządzania. Jak integracja z CEPIK ograniczyła ryzyko i usprawniła organizację pracy?

Integracja z CEPIK to przykład praktycznego wykorzystania Intranetu pod konkretne potrzeby organizacji.



Wywiad numeru

### Socjotechnika. Jak działają cyberoszuści i jak chronić się przed zagrożeniem z ich strony?

Istotnym elementem przeciwdziałania hakerom jest budowanie świadomości wśród pracowników i społeczeństwa.

## ■ Studium przypadku

# Od Intranetu do odpowiedzialnego zarządzania. Jak integracja z CEPiK ograniczyła ryzyko i usprawniła organizację pracy?

Intranet kojarzy się głównie z portalem pracowników, dostępnym dla nich po zalogowaniu i będącym miejscem dostępu do informacji. Jednak rola tego narzędzia może wykraczać poza typowy kanał komunikacji wewnętrznej, stając się praktycznym hubem organizacyjnym, korzystnym tak dla pracowników, jak i kadry zarządzającej. Doskonale pokazało to wdrożenie przeprowadzone w Zakładzie Wodociągów i Kanalizacji w Łodzi, gdzie Intranet stanowi rozwiązanie realnie wspierające procedury organizacji.

Dla wielu organizacji wyzwaniem okazuje się połączenie procesów wewnętrznych, związanych z zarządzaniem informacją, dostępem do dokumentacji i bezpieczeństwem operacyjnym. Wynika to z rosnącej liczby komunikatów, regulaminów i rozporządzeń, zmieniających się aktów prawnych, zróżnicowania procedur i rozproszenia danych pomiędzy wieloma systemami. Konieczne więc staje się stworzenie jednego miejsca, które poprzez integrację wspomnianych procesów zapewni faktyczne wsparcie w wykonywaniu codziennych obowiązków zawodowych. Takim miejscem może stać się Intranet, który nie powinien być już rozpatrywany wyłącznie w kategorii portalu komunikacji wewnętrznej, ale centralnego środowiska pracy – ułatwiającego dostęp do wiedzy, łączącego kluczowe procesy organizacyjne i wspierającego realizację codziennych obowiązków.

Z takiego założenia wyszło Przedsiębiorstwo Wodno-Kanalizacyjne, które świadome własnych potrzeb organizacyjnych i dostępnych możliwości technologicznych zdecydowało o wdrożeniu nowoczesnej wersji Intranetu. Istotne było, aby jego projekt odzwierciedlał strukturę organizacyjną przedsiębiorstwa, obowiązujące procedury i zakres przetwarzanych informacji. Równie ważny okazał się wybór samej platformy intranetowej, która musiała oferować funkcjonalności wpisujące się w założenia projektowe, a jedno-

cześnie zapewniać szerokie możliwości integracji z innymi systemami.

## Pierwszy etap, czyli strefa komunikacji

Motywacją do wdrożenia Intranetu była przede wszystkim potrzeba uporządkowania komunikacji wewnętrznej i stworzenia jednego, spójnego dostępu do informacji, a także systemów użytkowanych w organizacji.

**Nowoczesny Intranet nie jest już wyłącznie miejscem udostępniania informacji, ale praktycznym centrum organizacji pracy.**

Nie chodziło więc wyłącznie o uruchomienie klasycznego portalu pracowniczego, a o stworzenie praktycznego narzędzia pracy, które ułatwi centralizację dokumentów, odnajdywanie materiałów firmowych, usprawni obieg informacji i ograniczy rozproszenie danych. W związku z tym w ramach pierwszego etapu projektu uruchomiono rozwiązanie będące wewnętrznym centrum komunikacji i organizacji pracy. Tak powstały



Intranet przyjął formę praktycznego huba organizacyjnego, posiadającego funkcjonalności konieczne tak z perspektywy specjalistów HR, kadry zarządzającej oraz pracowników. Tym samym wyposażono go w m.in.: katalog dokumentów, wyszukiwarkę aktów prawnych, bazę kontaktów, informacje z obszaru cyberbezpieczeństwa, linki do systemów firmowych. Ważnym elementem tak skomponowanego zakresu funkcjonalnego stała się również opcja rezerwacji zasobów, takich jak pomieszczenia czy pojazdy służbowe.



## Drugi etap, czyli integracja z CEPiK

Szybko okazało się jednak, że potencjał platformy intranetowej jest znacznie większy, więc zdecydowano o rozszerzeniu roli Intranetu. Podyktowane było to charakterem działalności przedsiębiorstwa, gdzie część pracowników korzysta z pojazdów służbowych, w tym również pojazdów specjalistycznych o znaczącej wartości. W takim przypadku pracodawca musi mieć pewność, że osoby dopuszczone do prowadzenia pojazdów posiadają aktualne i wymagane uprawnienia.

**Integracja z CEPiK pokazała, że Intranet obok komunikacji wewnętrznej może też wspierać procesy związane z bezpieczeństwem, odpowiedzialnością i ciągłością działania.**

W rezultacie Intranet uzupełniono o moduł weryfikacji uprawnień kierowców, zintegrowany z Centralną Ewidencją Pojazdów i Kierowców. Dzięki temu procedura kontroli uprawnień osób prowadzących pojazdy służbowe została niemal całkowi-

cie zautomatyzowana. System cyklicznie sprawdza w bazie CEPiK statusy dokumentów, w tym zakresy uprawnień i terminy ważności, dla wszystkich zarejestrowanych kierowców. Wygenerowany na tej podstawie raport zawiera aktualne informacje o zmianach, przykładowo o zatrzymaniu prawa jazdy, zbliżającym się terminie wygaśnięcia dokumentu lub konkretnej kategorii uprawnień. Taka informacja trafia do osób odpowiedzialnych, co pozwala szybko reagować na sytuacje, które mogłyby mieć wpływ na bezpieczeństwo pracy, ciągłość operacyjną i odpowiedzialność pracodawcy.

Dzięki rozbudowie Intranetu o bardzo dziedziczny moduł zintegrowany z zewnętrznym rejestrem przedsiębiorstwo zyskało narzędzie ułatwiające kontrolę, zwiększające bezpieczeństwo i ograniczające ryzyko konsekwencji finansowych lub formalnych w przypadku losowych zdarzeń drogowych.

Ważnym aspektem projektu okazały się kwestie formalne związane z przetwarzaniem danych osobowych, które zostały obsłużone zgodnie z aktualnymi regulacjami. Platforma intranetowa została tak przygotowana, aby obowiązki wynikające z RODO mogły zostać właściwie zabezpieczone tak w przypadku utrzymania rozwiązania we własnej infrastrukturze, jak i w środowisku hostingowym dostawcy.

## Efekt, czyli korzyści dla wszystkich

Intranet wdrożony w ZWIK to przykład rozwiązania, którego korzyści należy rozpatrywać w szerokim wymiarze – pracownik, kierownik, specjalista HR i cała organizacja. Pokazuje, jak centralizacja komunikacji i integracja z zewnętrznymi rozwiązaniami może przełożyć się na lepszą kontrolę nad procesami i wyższy poziom bezpieczeństwa w przedsiębiorstwie.

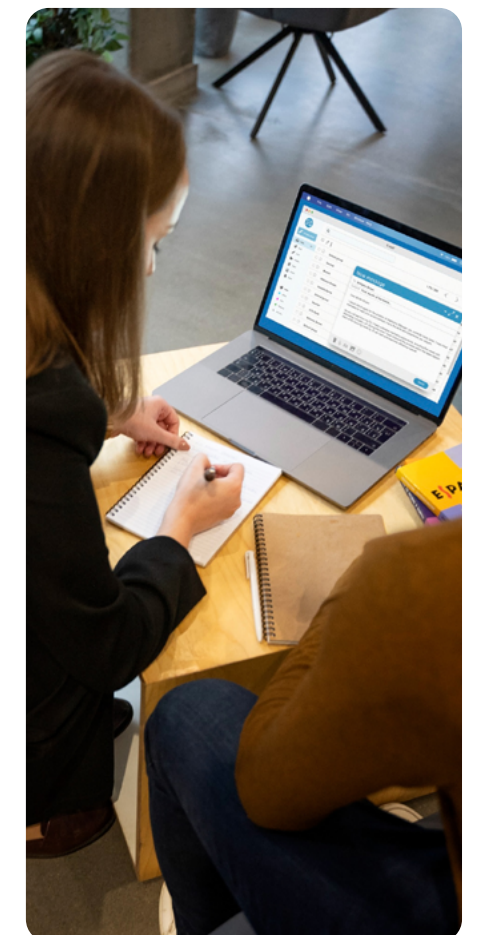
Pracownicy nie muszą już szukać informacji w wielu rozproszonych miejscach ani kontaktować się z różnymi działami, w szczególności z działem HR, w celu uzyskania dokumentacji czy też wyjaśnień w sprawach formalnych bądź organizacyjnych. Z kolei integracja z CEPiK pozwoliła zautomatyzować kontrolę uprawnień pracowników na stanowiskach kierowców i przypomina o zbliżających się ter-

minach wygaśnięcia, co zmniejsza ryzyko nieświadomego niedopełnienia przez nich obowiązków.



**Intranet traktowany jako jedno środowisko pracy pozwala szybciej podejmować decyzje, łatwiej utrzymać zgodność z procedurami i skuteczniej ograniczać ryzyko organizacyjne.**

Kierownicy i osoby odpowiedzialne za organizację pracy zyskali bieżący dostęp do aktualnych informacji dotyczących uprawnień kierowców, bez konieczności prowadzenia ręcznej, czasochłonnej weryfikacji. Dzięki temu mogą podejmować decyzje szybciej i z większą pewnością,





że pracownicy realizujący powierzone im zadania dysponują wymaganymi kwalifikacjami.

Jeśli chodzi o samą organizację, to istotną zaletą jest tu ograniczenie ryzyka organizacyjnego i finansowego. W przypadku przedsiębiorstw wykorzystujących pojazdy służbowe, zwłaszcza specjalistyczne i o wysokiej wartości, dopuszczenie do pracy osoby bez aktualnych uprawnień mogłoby skutkować poważnymi konsekwencjami.

Wartością dodaną projektu jest platforma intranetowa, którą można rozwijać wraz z potrzebami przedsiębiorstwa. Zbudowany na niej Intranet stał się centralnym środowiskiem pracy, do którego można dodawać kolejne moduły, funkcjonalności i integracje, na potrzeby obsługi nowych procesów, bez konieczności wdrażania odrębnych narzędzi. Dzięki temu organizacja zyskała nie tylko usprawnienia potrzebne w danym momencie, ale też bazę do dalszej cyfryzacji i optymalizacji działań.



Decydując się na wdrożenie Intranetu, od początku zakładaliśmy, że nie ma to być wyłącznie portal pracowników do wewnętrznej komunikacji, ale praktyczne narzędzie wspierające organizację pracy

w całym przedsiębiorstwie. Dlatego oprócz typowych funkcjonalności związanych z zarządzaniem informacją, postawiliśmy na rozwiązania istotne z punktu widzenia działu HR. Chodziło przede wszystkim o łatwiejszy dostęp do dokumentów, struktury organizacyjnej i systemów firmowych. Szybko jednak okazało się, że platforma intranetowa daje znacznie większe możliwości, więc kolejnym krokiem stał się moduł weryfikacji uprawnień kierowców. W kontekście prowadzonej działalności jest to szczególnie istotne dla sprawnego i bezpiecznego zarządzania flotą pojazdów. Przygotowana integracja Intranetu z bazą CEPIK pozwoliła automatycznie sprawdzać status i zakres uprawnień kierowców pojazdów służbowych, co ogranicza ryzyko ewentualnych, nieświadomych naruszeń prawnych.

**Karol Tyka**

Kierownik Wydziału Transportu – Zakład Wodociągów i Kanalizacji w Łodzi

## Cyfryzacja, ale z praktycznym podejściem

Dobrze zaprojektowany Intranet może, a nawet powinien rozwijać się razem z potrzebami organizacji. Projekt zrealizowany przez ZWIK to doskonały przykład tego, jak Intranet może ewoluować od kla-



Intranet powinien  
rozwijać się wraz  
z potrzebami organizacji.

sycznego portalu komunikacji wewnętrznej, poprzez praktyczne narzędzie HR, aż po rozwiązanie wspierające strategiczne procesy organizacji. Wykonana integracja z CEPIK w obszarze istniejącego już środowiska pokazała, jak dobrze i skutecznie wykorzystać Intranet do budowy specjalistycznego modułu, który odpowiada na bardzo konkretne potrzeby organizacji. Efektem takiego podejścia jest rozwiązanie, które pozytywnie przekłada się na efektywność pracy, lepszą kontrolę nad procesami i wyższy poziom bezpieczeństwa organizacji.



**Krzysztof Pliś**

Ekspert w dziedzinie nowych technologii. Pełni rolę doradczą, skupiając się głównie na obszarze administracji publicznej. Dzięki znajomości procedur zamówień publicznych pomaga instytucjom w efektywnym doborze innowacyjnych rozwiązań informatycznych.

# Jak Intranet z chatbotem zmieniają jakość zarządzania informacją HR?

Przeczytaj case study i poznaj efekty wdrożenia. Sprawdź, jak łatwo usprawnić komunikację HR.



Zeskanuj kod



**Pobierz bezpłatnie materiał**



# Odporność i niezależność. Suwerenność technologiczna administracji publicznej

Technologia i świat wirtualny stały się nieodłącznym elementem naszej codzienności. Bez wątpienia są też fundamentem funkcjonowania społeczeństw, państw czy światowej gospodarki. Systemy informatyczne wspomagają nas w ogromnej ilości zadań i podejmowanych przez nas decyzji, zarówno tych mało istotnych, jak i krytycznych. Są szeroko wykorzystywane w administracji publicznej – ciężko wyobrazić sobie dziś urząd, który potrafi funkcjonować bez IT. W zdigitalizowanym świecie, pytanie o to, kto kontroluje wykorzystywane technologie i przetwarzane w nich informacje, staje się pytaniem o naszą cyfrową niepodległość i bezpieczeństwo.

Suwerenność technologiczna nie oznacza całkowitej rezygnacji z rozwiązań dostarczanych z zewnątrz. Oznacza świadome ich wykorzystanie przy jednoczesnym utrzymaniu zdolności do podejmowania niezależnych decyzji oraz kontroli nad kluczowymi obszarami naszej codzienności. Choć to proces niezwykle trudny w świecie zdominowanym przez big tech, to nie znaczy, że jest nieosiągalny. Wymaga po prostu szerokiego spojrzenia i wielowątkowego podejścia.

## Suwerenność globalna i lokalna

Suwerenność na poziomie globalnym nie dotyczy jedynie aspektu kontroli i zarządzania usługami IT, a stanowi istotny element budowy przewagi geopolitycznej i gospodarczej. Żadne państwo nie jest dziś w całości samowystarczalne technologicznie i odcięcie się od globalnej współpracy nie jest faktycznym i możliwym rozwiązaniem. Dla dostawców krytycznych technologii może to oznaczać istotny atut w innych, niezwiązanych z tym wątkiem aspektach. Unikanie technologicznego impasu możliwe jest więc poprzez ograniczanie jednostronnych i krytycznych zależności. W praktyce sprowadza się to do dywersyfikacji rozwiązań, dostawców i współprac.

W środowiskach lokalnych suwerenność jest rozumiana w nieco inny spo-

sób. Sprowadza się ona do minimalizacji ryzyk związanych z brakiem pełnej kontroli nad strategicznymi procesami. Ryzyka te mogą bezpośrednio lub pośrednio wpływać na społeczności, powodując zakłócenia w działaniu usług o określonym poziomie krytyczności.

## Zależność jako źródło zagrożeń

Korzystanie z zewnętrznych rozwiązań nie jest błędem samym w sobie. Choć zależność technologiczna stanowi naturalną i akceptowalną konsekwencję dynamicznej cyfryzacji, to uzależnienie od konkretnego narzędzia jest zjawiskiem niebezpiecznym, którego należy unikać.

**Suwerenność technologiczna nie oznacza odcięcia się od zewnętrznych rozwiązań, lecz świadome zarządzanie zależnościami, dostawcami, danymi i ryzykiem utraty kontroli nad kluczowymi procesami.**



Istnieje szereg ryzyk, które może generować taka sytuacja. Wśród nich najbardziej podstawowym zagrożeniem okazuje się ryzyko naruszenia ciągłości działania. Jeśli krytyczny proces bądź usługa są zależne od zewnętrznego dostawcy, to naturalnie może on wpłynąć na ich dostępność. Innym zagrożeniem może być zjawisko vendor lock-in, a więc sytuacja, w której odbiorca traci akceptowalną kosztowo możliwość wyjścia z ekosystemu wybranego producenta. Taka sytuacja może generować także dług technologiczny, jeżeli narzędzia dostarczane przez tego dostawcę nie odpowiadają na faktyczne potrzeby jednostki, co w konsekwencji może prowadzić do utraty zdolności bądź kompetencji w danym obszarze, np. do zarządzania IT wtedy, kiedy zadanie to było powierzone zewnętrznemu dostawcy.

Naturalnie, nie bez znaczenia jest również warstwa faktycznej lokalizacji danych i dostępu do nich. W przypadku usług wyniesionych należy mieć świadomość ograniczeń w obszarze zarządzania zabezpieczeniami fizycznymi. Oczywiście, nie oznacza to utraty kontroli nad danymi w przypadku wyboru usług chmurowych, jednak w takim scenariuszu, unikając odpowiedzialności za fizyczne bezpieczeństwo środowiska, zyskujemy nową pulę ryzyk związaną z brakiem pełnej kontroli nad dostępem do danych.

Suwerenność cyfrowa jest również czę-

kalnych jednostkach i dlatego właściwe praktyki chroniące przed utratą kontroli nad swoim środowiskiem stanowią jeden z wymogów znowelizowanego Krajowego Systemu Cyberbezpieczeństwa.

**Dla administracji publicznej cyfrowa niezależność zaczyna się lokalnie, od wiedzy o używanych systemach, krytycznych usługach, dostawcach i możliwościach ich zmiany w razie potrzeby.**

sto łączona z ryzykiem wynikającym z dynamiki w wymiarze prawnym i regulacyjnym. Zaburzenie relacji między narodowych między państwami dostawcy a odbiorcy tworzy niebezpieczeństwo braku możliwości współpracy wskutek ograniczeń zdefiniowanych na poziomie lokalnych bądź globalnych przepisów prawa, a w skrajnych przypadkach również np. embarga.

Szeroki wachlarz zagrożeń i ryzyk związanych z brakiem kontroli nad pochodzeniem stosowanej technologii sprawia, że suwerenność cyfrowa stanowi dziś jeden z najbardziej istotnych tematów rozpatrywanych w kontekście cyberbezpieczeństwa, zaś jej znaczenie w skali globalnej sprowadza dyskusję na poziom bezpieczeństwa państw i społeczeństw. To wystarczający powód, aby zadbać o suwerenność technologiczną w naszym, lokalnym ekosystemie.

## Urząd suwerenny technologicznie

Choć dla administracji publicznej widmo globalnych konsekwencji braku suwerenności może wydawać się nieco odległe, to w rzeczywistości „public” stanowi podstawowy obszar zainteresowań atakujących. Cyberszpiegostwo, ataki destrukcyjne czy naruszenie terytorium cyfrowego to działania adresowane właśnie do urzędów i jednostek im podległych. Globalna suwerenność budowana jest w lo-

konkretnego rozwiązania powinny być znane, zdefiniowane i zaakceptowane.

Bezpieczny łańcuch dostaw będzie odpowiedzialnością na rozwój i zmiany, jakie w czasie będą realizowane przez nasz urząd. Z uwagi na to, że ochrony potrzebujemy już dziś, warto również przeanalizować naszą sytuację w tym momencie. Do kontroli niezbędna będzie pełna inwentaryzacja zasobów, która odpowie nam na pytanie, z jakich środków korzystamy do świadczenia konkretnych usług. Spis zasobów, aktywów i procesów stanowi integralną część analizy ryzyk, więc odśledzenie tych danych nie powinno stanowić problemu. Informacja taka pozwoli nam na selekcję zadań krytycznych, na których powinniśmy się skupić w dalszej części analizy. Na tym etapie należy ustalić, czy i w jakim zakresie procesy te zależą od dostawców. Warto mieć na uwadze, że często pojedyncza usługa może obsługiwać szereg procesów, które jedynie pośrednio wpływają na świadczone przez nas usługi. Wykrycie tych zależności jest niezbędne do właściwej definicji krytyczności dostarczanych nam usług. Dopiero tak zebrane dane pozwolą na ocenę naszej technologicznej samowystarczalności.

Jak stworzyć suwerenny urząd? Odpowiedzią jest budowa odporności w zakresie łańcucha dostaw. Świadomy wybór rozwiązań oraz ich kontrola w czasie pozwolą nam na utworzenie środowiska informatycznego, które nie będzie generowało zbędnych zależności. W naszym długofalowym planie rozwoju powinniśmy więc przeanalizować, czy wybrana i planowana do wdrożenia technologia może być reprezentowana przez różnych, faktycznie odmiennych od siebie dostawców. Należy także zweryfikować, czy realizowane i planowane wdrożenia nie uniemożliwią nam późniejszej zmiany dostawcy, np. ze względu na konieczne do utworzenia integracje. Analizie powinien podlegać nie tylko aspekt techniczny, ale także uwarunkowania operacyjne czy ekonomiczne. Ograniczenia i zagrożenia powstałe wskutek wyboru

**Największym zagrożeniem nie jest samo korzystanie z zewnętrznych technologii, ale brak świadomości, jak głęboko organizacja jest od nich zależna i jakie skutki przyniosłaby ich niedostępność.**





Czy utrata dostawcy bądź opóźnienie w dostawie wpłynie na naszą zdolność świadczenia usług? Czy proces zakupu obejmuje weryfikację bezpieczeństwa dostawców? Czy znamy koszty utrzymania, migracji i zmiany systemu? Czy mamy możliwość zmiany dostawcy w dowolnym momencie? Czy podpisane umowy gwarantują nam akceptowalny poziom bezpieczeństwa i niezależności?

To tylko część z kluczowych pytań, na które należy znaleźć odpowiedź. Tam, gdzie będzie ona negatywna, powinniśmy wprowadzić szereg działań naprawczych lub, jeśli nie ma takiej możliwości, zdefiniować, udokumentować i zaakceptować zależność po to, żeby przy kolejnej iteracji wrócić do tego wątku i ponownie przeanalizować potencjalne sposoby wyjścia z technologicznego impasu, w którym się znaleźliśmy.

### Wartością urzędu są dane

Suwerenność powinna być rozumiana również na poziomie samej pracy z danymi. Obok weryfikacji środowiska informacyjnego niezbędna jest dokładna analiza płaszczyzny, w jakiej przetwarzamy informacje. Jeśli wykorzystujemy w tym celu środowiska zewnętrzne, to należy ocenić również naszą niezależność tam, gdzie nie jesteśmy właścicielami zasobów.

Czy mamy pełną wiedzę, gdzie fizycz-

nie zlokalizowane są dane? Czy dostawca określa udział firm trzecich w procesie świadczenia usługi? Czy system przewidywa możliwość pełnego eksportu danych w otwartym, możliwym do odtworzenia formacie? Czy dostawca gwarantuje nam możliwość całkowitego usunięcia informacji po zakończeniu współpracy?

Dokładna i rzetelna ocena zarówno warstwy wewnętrznej, jak i zewnętrznej wskazuje faktyczny poziom suwerenności technologicznej.

### Suwerenność jako element bezpieczeństwa

Urząd możemy uznać za suwerenny technologicznie nie wtedy, kiedy korzysta jedynie z krajowych technologii ulokowanych w lokalnym data center, a wtedy, kiedy jest świadomy swoich zależności i ograniczeń wynikających z zewnętrznej



**Świadomość zależności i umiejętność zarządzanie zewnętrzną współpracą to ważny aspekt suwerenności technologicznej.**

✓  
Suwerenność  
cyfrowa i podniesienie  
cyfrowego  
bezpieczeństwa.

współpracy, a ponadto potrafi nimi zarządzać. Jednostka, która zna swoich dostawców, posiada zdolność do ich zmiany w razie potrzeby i dysponuje własnymi kompetencjami, będzie w stanie realizować zadania publiczne nawet w dynamicznym i zmiennym świecie pełnym wielowarstwowych zagrożeń. Budowa cyfrowej niezależności jest więc długotrwałym procesem, który stanowi element zarządzania cyberbezpieczeństwem w organizacji.



**Norbert Nowak**

Ekspert cyberbezpieczeństwa. Zajmuje się realizacją usług związanych z analizą i projektowaniem infrastruktur pod kątem ochrony systemów i danych. Zrealizował liczne projekty w zakresie networkingu, storage'u, wirtualizacji oraz bezpieczeństwa IT. Prelegent i panelista konferencji branżowych, a także autor publikacji dziedzinowych.

# NARZĘDZIOWNIK AI 3.0 REVOLUTIONS

Od pierwszego promptu do mistrzostwa w używaniu narzędzi AI

- # 20 sesji na żywo x 2 godz.
- # Dostęp do nagrań na zawsze
- # Ćwiczenia utrwalające wiedzę
- # Zamknięty serwer Discord
- # Bogaty zestaw dodatków (gotowe rozwiązania, wdrożenia, checklisty)
- # Certyfikaty ukończenia szkolenia



START JUŻ 24.09.2026 R.

ZAPISZ SIĘ: [NAI.SEKURAK.PL](https://nai.sekurak.pl)

# Samoobsługa pracownicza. Cyfrowe rozwiązanie, które usprawnia kadry w urzędzie

W dobie postępującej cyfryzacji administracji publicznej, jednym z kluczowych wyzwań staje się modernizacja wewnętrznych procesów administracyjnych. Tradycyjne metody zarządzania dokumentacją kadrową, oparte na papierowych wnioskach i ręcznym wprowadzaniu danych, stają się nieefektywne i kosztowne. Odpowiedzią na te potrzeby jest system Teta HR, oferowany przez firmę OPTeam, który w połączeniu z portalem samoobsługowym Teta ME, rewolucjonizuje sposób funkcjonowania działów kadr i płac w sektorze publicznym.

Dla wielu instytucji publicznych barierą we wdrażaniu nowoczesnych systemów IT były dotychczas wysokie koszty infrastruktury oraz długotrwałe procesy implementacji. Sytuacja jednak uległa zmianie i obecnie na rynku dostępna jest alternatywa dla uruchomienia oprogramowania w oparciu o własne zasoby serwerowe.

## Cyfrowa transformacja w modelu SaaS

Rozwiązaniem jest udostępnienie systemu Teta HR w modelu SaaS (Software as a Service). W tym modelu oprogramowanie działa w chmurze, co eliminuje konieczność zakupu drogich serwerów, licencji na bazy danych czy utrzymywania rozbudowanych zespołów IT do obsługi systemu.



**System HR w modelu SaaS można uruchomić już w sześć miesięcy bez inwestowania w zasoby serwerowe.**

Wdrożenie w modelu SaaS pozwala na znaczne skrócenie czasu uruchomienia systemu – w przypadku wersji prekonfigurowanej może to potrwać zaledwie

do sześciu miesięcy. Jest to rozwiązanie szczególnie dedykowane mniejszym i średnim instytucjom sektora publicznego, takim jak jednostki samorządu terytorialnego, spółki miejskie (MPWiK, MPO, ZTM) czy ciepłownie, zatrudniającym do tysiąca pracowników. Dzięki temu zyskują one dostęp do narzędzi klasy ERP, które wcześniej były domeną jedynie największych organizacji.

## Biuro w smartfonie pracownika

Sercem nowoczesnej samoobsługi jest aplikacja Teta ME (Mobile Edition), która zapewnia pracownikom i kierownikom całodobowy dostęp do procesów HR z poziomu przeglądarki internetowej lub urządzeń mobilnych. Cyfryzacja tych procesów sprawia, że dane wprowadzone przez pracownika w portalu natychmiast trafiają do głównej bazy danych systemu kadrowo-płacowego, co zapewnia ich spójność i eliminuje błędy wynikające z ręcznego przepisywania informacji.

**Najważniejsze funkcjonalności portalu dla pracownika obejmują:**

➤ **Mój profil**

Stały wgląd w aktualne dane kadrowe, informacje o wynagrodzeniu, zgłoszonych członkach rodziny czy powierzonym wyposażeniu, takim jak laptop czy telefon służbowy.



➤ **Elektroniczne wnioski**

Możliwość samodzielnego wnioskowania o aktualizację numeru rachunku bankowego, zmianę adresu zamieszkania czy złożenie deklaracji dotyczących PPK i wiele innych wniosków kadrowych (w tym ZFŚS).

➤ **Obsługa dokumentów płatniczych**

Pracownicy mają dostęp do swoich paszów płacowych oraz deklaracji PIT-II. Co istotne, pobranie dokumentu PIT w systemie jest równoznaczne z elektronicznym potwierdzeniem jego odbioru, co zdejmuje z działu kadr obowiązek drukowania i ręcznego dostarczania formularzy.

➤ **E-teczka**

Dostęp do zdigitalizowanej teczek pracowniczej, zawierającej świadectwa pracy, dyplomy czy orzeczenia, w pełni zgodnie z aktualnymi przepisami prawa.

## Automatyzacja czasu pracy i urlopów

Jednym z najbardziej czasochłonnych zadań w urzędach jest ewidencja i rozliczanie czasu pracy. System Teta HR automatyzuje te procesy, oferując moduł Rozliczanie Czasu Pracy, który kontroluje zgodność grafików z Kodeksem pracy. W obszarze planowania urlopów system

zapewnia pełną przejrzystość. Pracownik w każdej chwili widzi swój aktualny limit urlopowy oraz historię złożonych wniosków. Składanie wniosku odbywa się elektronicznie, a system automatycznie waliduje go pod kątem dostępnych dni i harmonogramu pracy. Przełożony może akceptować wnioski pojedynczo lub grupowo, również za pomocą aplikacji mobilnej, co drastycznie skraca czas obiegu dokumentów.

Unikalną funkcjonalnością jest tzw. „malarz dni”, który pozwala kierownikom na szybkie i intuicyjne tworzenie grafików pracy dla całych zespołów. System na bieżąco sygnalizuje ewentualne naruszenia wielu norm, np. odpoczynku czy średniotygodniowego wymiaru czasu pracy, co pozwala uniknąć błędów prawnych już na etapie planowania.

## Wsparcie dla kadry zarządzającej

Samoobsługa pracownicza w wydaniu Teta HR to także potężne narzędzie dla menedżerów. Dzięki modułom menedżerskim mogą oni sprawnie zarządzać zespołem poprzez:

➤ **Zlecenie i rozliczanie nadgodzin**

System pozwala na grupowe zlecenie pracy w nadgodzinach (np. w przypadku awarii) oraz monitorowanie ich odbioru, co generuje wymierne oszczędności finansowe.

➤ **Wnioski menedżerskie**

Możliwość elektronicznego wnioskowania o zatrudnienie nowej osoby, zmianę warunków umowy czy przyznanie podwyżki. Proces ten oparty jest na konfigurowalnym obiegu workflow, który może obejmować akceptację dyrektorów, kontroli budżetowej czy zarządu.

➤ **Analityka i raportowanie**

Kierownicy mają dostęp do dynamicznych raportów dotyczących absencji, stanu wykorzystania urlopów, terminów kończących się badań okresowych czy szkoleń BHP w swoich zespołach.

## Bezpieczeństwo danych i zgodność prawna

W sektorze publicznym kwestie bezpieczeństwa danych osobowych są priorytetem. System Teta HR w modelu SaaS zapewnia najwyższe standardy ochrony, zgodnie z wymogami RODO oraz dyrektywy NIS2. Dane są przechowywane w profesjonalnych centrach danych zlokalizowanych na terenie Polski, co gwarantuje, że nie opuszczają one obszaru jurysdykcji UE.

Regularne aktualizacje systemu gwarantują jego stałą zgodność ze zmieniającymi się przepisami prawa podatkowego, ubezpieczeniowego czy prawa pracy. Dzięki temu urzędy nie muszą martwić się o dostosowanie narzędzi do nowych stawek podatkowych czy zmian w zasadach naliczania zasiłków.

## Korzyści dla instytucji publicznej

Wdrożenie samoobsługi pracowniczej przynosi szereg korzyści, które przekładają się na sprawniejsze funkcjonowanie całego urzędu. Pierwsza to oszczędność czasu, dzięki automatyzacji powtarzalnych czynności, która odciąża dział HR, pozwalając specjalistom skupić się na bardziej merytorycznych zadaniach. Druga to redukcja kosztów, wynikająca z rezygnacji z papierowej dokumentacji, braku konieczności inwestycji we własną infrastrukturę IT oraz optymalizacji rozliczania nadgodzin. Trzecia to efektywność, ponieważ decentralizacja wprowadzania

danych (przez pracowników) przyspiesza procesy, np. zamknięcie miesiąca i naliczenie list płac. I czwarta to minimalizacja ryzyka pomyłek. Systemowe walidacje i automatyczny przepływ danych eliminują błędy ludzkie towarzyszące manualnej obsłudze dokumentów.

## Nowoczesne kadry w cyfrowym urzędzie

Podsumowując, system Teta HR w modelu SaaS wraz z portalem pracowniczym Teta ME to kompleksowe rozwiązanie, które pozwala instytucjom publicznym na szybki skok technologiczny. Dzięki cyfryzacji procesów kadrowo-płacowych jednostka samorządu terytorialnego, spółka miejska czy inny podmiot tego sektora staje się bardziej przyjazny dla pracownika, efektywniejszy dla menedżera i tańszy w utrzymaniu dla podatnika. To fundament nowoczesnej, cyfrowej administracji, w której technologia służy optymalizacji codziennej pracy, usprawnieniu obiegu informacji, zwiększeniu przejrzystości działań oraz lepszemu wykorzystaniu czasu i zasobów całej organizacji.



**Tomasz Dobrzański**

Ekspert w zakresie rozwiązań informatycznych w obszarze HR, księgowości i finansów. Posiada znajomość procedur kadrowo-płacowych i najnowszych technologii, które łączy z wieloletnim doświadczeniem na potrzeby optymalizacji procesów personalnych w organizacjach. Swoją wiedzę dzieli się jako prelegent i panelista podczas branżowych konferencji.

## Kultura organizacyjna w jednostkach samorządu terytorialnego

Współczesne cyberataki to bardzo zaawansowane i wieloetapowe procesy. MITRE ATT&CK wskazuje aż 15 etapów ataku, z których każdy może być reprezentowany przez szereg odrębnych technik stosowanych przez cyberprzestępców. Jedną z kluczowych faz jest „Initial Access”, a więc moment, w którym atakujący próbuje uzyskać dostęp do wewnętrznych zasobów urzędu.

Szacuje się, że w 2025 roku niemal 80% wszystkich skutecznych ataków w fazie „wejścia” wykorzystywało różne odmiany socjotechniki. Cyberprzestępcy świadomie rezygnowali z forsowania zabezpieczeń technicznych i wpływali na użytkowników tak, żeby to od nich, nieświadomych, zagrożenia uzyskać niezbędne poświadczenia. Najpopularniejszą formą socjotechniki jest phishing, a więc oszustwo wykorzystujące komunikację z użytkiem poczty elektronicznej. Warto jednak zaznaczyć, że metod jest znacznie więcej i mogą one wykorzystywać także inne media komunikacyjne czy nawet interakcję fizyczną. Niezależnie od metody, wszystkie mają wspólny cel – oszukać użytkownika i przekonać go do przekazania danych.

Jedną z wielu przewag człowieka nad maszyną jest jego umiejętność do niesablonowych zachowań. Dostosowujemy swoje decyzje do sytuacji, w której w danym momencie się znajdujemy. Choć często stanowi to ogromny atut, to w procesie budowania bezpieczeństwa nie jest to szczególnie pożądana cecha.



**Świadomość, powtarzalne procedury i dobre nawyki są równie ważne jak zabezpieczenia techniczne.**

Łatwiej chronić system, który niezależnie od okoliczności podąża za zaprogramowanymi instrukcjami niż człowieka, którego ścieżka osiągnięcia celu może zostać zaburzona czynnikami zewnętrznymi. I niestety ta „właściwość” użytkownika decyduje o wysokiej skuteczności inżynierii społecznej i utrudnia skuteczną ochronę przed socjotechniką. Nie jesteśmy jednak bezsilni. Istnieje szereg metod, które pomagają zbudować wysoką świadomość użytkowników końcowych i wdrożyć w ich codziennej pracy standard, który będzie ograniczał ryzyko skutecznego ataku. Najbardziej popularnym narzędziem są szkolenia z cyberbezpieczeństwa oraz kampanie socjotechniczne.

### Szkolenia z cyberbezpieczeństwa

Właściwa organizacja szkoleń skupi uwagę uczestników i pozwoli im nabyć niezbędną wiedzę na temat podstawowych form zagrożeń, z jakimi mogą spotkać się w codziennej pracy. Odpowiedni i dobrany do odbiorców zakres tematyczny oraz interaktywna forma spotkania z trenerem decydują o sukcesie szkolenia, które powinno być również regularnie powtarzane tak, aby użytkownicy zawsze mieli dostęp do aktualnych informacji. Jednocześnie, zbyt długie i rozbudowane tematycznie szkolenia zniechęcają uczestników do poszerzania wiedzy w tym istotnym temacie i mogą negatywnie wpłynąć na ich zdolności do ochrony. Sposób prowadzenia szkole-



nia, zaawansowanie techniczne, długość i częstotliwość to kluczowe wskaźniki, które powinniśmy dopasować do naszych pracowników tak, żeby spotkanie faktycznie przyniosło wyznaczony cel.

### Kampania socjotechniczna

Zyskująca na popularności metoda weryfikacji świadomości użytkowników końcowych to zderzenie ich z faktycznym zagrożeniem w formie symulowanej kampanii socjotechnicznej.



**Symulowana kampania socjotechniczna pozwala sprawdzić, jak w sytuacji zagrożenia zareaguje zespół.**

Taki próbny atak może przyjąć formę prostego phishingu, rozmowy telefonicznej (vishingu) lub próby nieautoryzowanego wtargnięcia do stref bezpiecznych w urzędzie, np. do archiwum. Symulacja pozwoli nam sprawdzić, jak zachowa się nasz zespół wtedy, kiedy faktycznie dojdzie do ataku. Nie oceniamy jednak wyłącznie faktu sukcesu lub porażki pró-

domość ich znaczenia w systemie zabezpieczeń i poczucie współodpowiedzialności za ochronę zasobów urzędu. Użytkownik, któremu nie zależy na bezpieczeństwie przetwarzanych informacji, nie będzie dążył do utrzymania ich spójności i integralności, a swoje działania w tym zakresie ograniczy jedynie do niezbędnego minimum wymaganego wewnętrznymi procedurami. Kultura bezpieczeństwa to informacja, jaką urząd przekazuje swoim pracownikom, mówiąca o tym, że „bezpieczeństwo to nie problem działu IT czy zarządu, bezpieczeństwo to nasz wspólny cel”.

### Przykład idzie z góry

Zbudowanie kultury bezpieczeństwa to długi i skomplikowany proces. Niezwykle istotnym jego punktem jest zaangażowanie najwyższego kierownictwa. Pracownicy obserwują kadrę zarządzającą i jeśli widzą, że ich przełożeni czynnie angażują się w ochronę danych, aktywnie uczestniczą w szkoleniach i faktycznie dbają o ochronę zasobów, to sami również będą podążać ich śladem. Innym istotnym elementem jest sposób zarządzania incydentami.



**Skuteczność cyberbezpieczeństwa zależy od codziennych decyzji pracowników, jasnych procedur i kultury organizacyjnej, w której każdy rozumie swoją rolę w ochronie danych.**

Jeśli pracownik popełni błąd, w wyniku którego dojdzie do naruszenia, ale zgodnie z procedurami podejmie wszystkie niezbędne do jego minimalizacji kroki, a mimo to spotkać go dotkliwe konsekwencje, to przy kolejnym takim zdarzeniu będzie dążył do ukrycia swojego błędu, opóźniając w ten sposób reakcję i realnie działając na niekorzyść jednostki. Często obserwowanym błędem jest także duże rozproszenie proceduralne i skomplikowane zasady. Spotykając się z potencjalnym incydentem, zestresowany pracownik nie wie, czy lepiej naj-

pierw poinformować bezpośredniego przełożonego, dział IT, najwyższe kierownictwo czy samodzielnie podejmować interwencję i kontaktować się z policją lub CSIRT. W efekcie jego reakcja może być nieprawidłowa, opóźniona bądź zupełnie zaniechana, szczególnie wtedy, kiedy wykryje zdarzenie, ale nie jest pewien, czy jest to faktyczny incydent, np. widzi nieznaną mu osobę w strefie bezpiecznej, do której w teorii nie powinna ona mieć dostępu.

### Dobre praktyki podstawą

Warto rozważyć również wewnętrzną promocję i zachętę do realizacji tych dobrych praktyk. Jeśli pracownicy dostrzegą, że proaktywna postawa jest nagradzana, niemal naturalnie powstanie forma wewnętrznej rywalizacji, w której pracownicy będą chętniej angażować się w bezpieczeństwo i aktywniej reagować na potencjalne incydenty. Budowanie kultury bezpieczeństwa i świadomości pracowników to niezwykle istotny proces, który dobrze przeprowadzony może w ogromnym stopniu wpłynąć na zdolność naszej organizacji do odpięrania cyberataków. Warto więc już dziś zaplanować kolejne działania w tym zakresie.



**Norbert Nowak**

Ekspert cyberbezpieczeństwa. Zajmuje się realizacją usług związanych z analizą i projektowaniem infrastruktury pod kątem ochrony systemów i danych. Zrealizował liczne projekty w zakresie networkingu, storage'u, wirtualizacji oraz bezpieczeństwa IT. Prelegent i panelista konferencji branżowych, a także autor publikacji dziedzinowych.

# Zastosowania sztucznej inteligencji w jednostkach samorządu terytorialnego

Jak wynika z raportu NASK-PIB AI w e-administracji publicznej, zdecydowana większość urzędników dostrzega potencjał sztucznej inteligencji w usprawnianiu codziennej pracy. Polska Polityka Rozwoju Sztucznej Inteligencji do 2030 roku wprost wskazuje, że polskie samorządy odgrywają dużą rolę w efektywnym rozwoju AI w administracji, a programy pilotażowe w jednostkach samorządu terytorialnego są już prowadzone i będą kontynuowane w kolejnych latach. Jakże więc obszary, w których sztuczna inteligencja sprawdzi się najlepiej dla JST?

Wśród najczęściej wymienianych obszarów zastosowania AI w JST wskazuje się te związane z obsługą formalności i mieszkańców, pracą biurową i legislacyjną, weryfikacją informacji i dokumentów, a nawet analityką danych.

## Automatyzacja procesów administracyjnych

Jednym z najbardziej naturalnych zastosowań AI w JST jest automatyzacja powtarzalnych procesów biurowych. W obliczu malejącej liczby pracowników administracyjnych, szczególnie na stanowiskach pomocniczych i urzędniczych, systemy sztucznej inteligencji mogą przejąć część rutynowych zadań, pozwalając dostępnej kadrze skupić się na pracy wymagającej bezpośredniego zaangażowania człowieka.

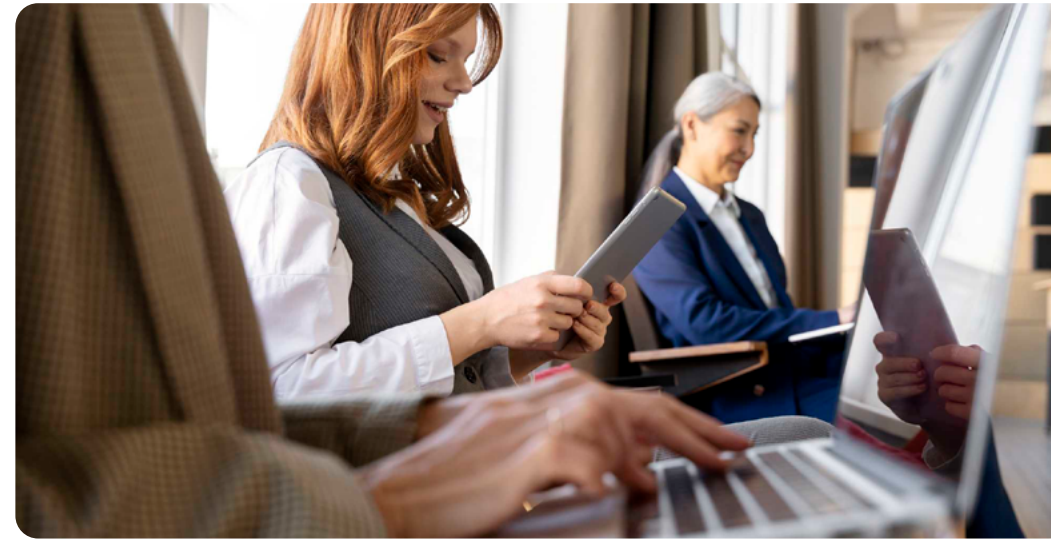
Dotyczy to w szczególności rejestracji korespondencji przychodzącej, automatycznej dekretacji pism na właściwe komórki organizacyjne, archiwizacji dokumentów i nadawania sygnatur, a także monitorowania postępu spraw i generowania raportów. Ponad 61% urzędników ankietowanych przez NASK-PIB pozytywnie oceniło możliwość wsparcia AI w zakresie monitorowania postępu spraw i raportowania. Co istotne, badani wskazywali, że automatyzacja obiegu dokumentów jest szczególnie wartościowa przy sorto-

waniu i dekretacji korespondencji, a automatyczna rejestracja korespondencji przychodzącej i ewentualnie dekretacja na poszczególne komórki znacznie ułatwiłaby pracę – jak wprost wyrażali się urzędnicy uczestniczący w badaniach jakościowych.

## Wyszukiwanie informacji i analiza dokumentów

Pracownicy samorządowi codziennie zmagają się z koniecznością wyszukiwania informacji w rozbudowanych bazach dokumentów – aktach prawnych, zarządzeniach, decyzjach administracyjnych, dokumentacji BIP czy wewnętrznych procedurach. Jest to jeden z najbardziej czasochłonných aspektów pracy urzędniczej, a zarazem obszar, w którym AI może przynieść największe i najszybsze korzyści.

AI może odciążyć pracowników urzędu od powtarzalnych zadań, pozwalając im skupić się na pracy wymagającej bezpośredniego zaangażowania człowieka.



Narzędzia oparte na przetwarzaniu języka naturalnego (NLP) pozwalają przeszukiwać ogromne zasoby dokumentacyjne poprzez pytania zadawane w języku potocznym – tak jak rozmawia się z asystentem. Badania NASK-PIB wskazują, że blisko dwie trzecie respondentów oceniło tę funkcjonalność jako zdolną znacząco wesprzeć pracę urzędników. Wartość tego rozwiązania jest szczególnie wyraźna przy przeszukiwaniu dużych zbiorów dokumentów, z którymi urzędnicy mają mniejszą styczność, a AI może łatwiej do nich dotrzeć i wyciągnąć z nich potrzebne w danym momencie informacje.

## Wirtualni asystenci AI wsparciem w obsłudze mieszkańców

Relacja urząd-obywatel stanowi serce działalności samorządowej. To właśnie tutaj sztuczna inteligencja w postaci chatbotów może przynieść wymierną poprawę jakości usług publicznych. Konwersacyjne systemy AI są w stanie obsługiwać typowe zapytania mieszkańców przez całą dobę, kierować ich do właściwych komórek organizacyjnych, informować o wymaganych dokumentach i procedurach, a nawet umożliwiać rezerwację terminów w urzędzie.

Na poziomie krajowym Polska zbudowała własne zaplecze: model językowy PL-

LuM dostosowany do polskich realiów prawnych i kulturowych oraz Wirtualnego Asystenta w aplikacji mObywatel. Celem tych rozwiązań jest, by użytkownicy mogli szybciej uzyskiwać odpowiedzi na pytania związane z procedurami urzędowymi.

Wirtualni asystenci AI mogą wspierać obsługę mieszkańców przez całą dobę, ułatwiając kontakt z urzędem.

## Zarządzanie miastem i infrastrukturą

Wraz z rozwojem Internetu Rzeczy (IoT) miasta generują coraz więcej danych z czujników, kamer, systemów transportu, wodociągów i energetyki. Sztuczna inteligencja, integrując te strumienie danych w czasie rzeczywistym, może stać się narzędziem zarządzania miastem nowej generacji. W zakresie transportu algorytmy AI są w stanie analizować dane o ruchu w czasie rzeczywistym, optymalizować przepływ pojazdów i przewidywać potencjalne zatory, umożliwiając proaktywne zarządzanie ruchem drogowym. Natomiast systemy predyktcyjne wspierające gospodarkę komunalną pozwalają na

lepsze zarządzanie odpadami, zużyciem energii i zasobami wodnymi. Nie bez znaczenia jest też obszar cyberbezpieczeństwa – algorytmy AI mogą wykrywać anomalie w sieciach infrastruktury krytycznej i reagować na potencjalne zagrożenia, zanim wyrządzą szkodę.

## Tworzenie treści

Generatywna sztuczna inteligencja – zdolna do tworzenia tekstów, tłumaczeń i streszczeń – otwiera nowe możliwości w zakresie pracy z dokumentami urzędowymi. Ponad 62% urzędników biorących udział w badaniu NASK-PIB wyraziło pozytywną opinię o zastosowaniu AI do tworzenia dokumentów urzędowych, a 77% przychylnie odniosło się do możliwości wsparcia w tłumaczeniu i redakcji treści w językach obcych.

W praktyce AI może pomagać w redakcji projektów pism, odpowiedzi na wnioski, raportów i protokołów, dbając o korektę językową, spójność stylistyczną i formatowanie. Szczególnie cenne jest jej zastosowanie do upraszczania języka urzędowego – nierzadko hermetycznego i niezrozumiałego dla przeciętnego obywatela.



## Wyzwania we wdrażaniu AI

Mimo obiecującego potencjału, wdrażanie AI w JST napotyka na liczne bariery. Badanie Ministerstwa Cyfryzacji przeprowadzone pośród ponad 8000 urzędników jednoznacznie wskazuje, że aż 82% z nich uznaje brak wiedzy i umiejętności za istotną lub bardzo istotną przeszkodę. Co szczególnie wymowne, prawie 60% ankietowanych określa swoją wiedzę o AI jako elementarną, a zaledwie 3% posiada zaawansowaną znajomość tematu.

Do istotnych barier należą też: niejasne lub brakujące regulacje prawne dotyczące AI w urzędach (wskazywane przez 73% respondentów), niedostateczne zasoby finansowe (62%), niewystarczająca infrastruktura techniczna (59%) oraz obawy dotyczące ochrony danych osobowych i zgodności z RODO. Warto przy tym podkreślić, że bariera kompetencyjna jest jednocześnie szansą – aż 93% ankietowanych urzędników zadeklarowało chęć podniesienia swoich kompetencji w zakresie AI, co tworzy idealne środowisko dla skutecznych programów edukacyjnych.

### Źródła

- NASK-PIB, AI w e-administracji publicznej, <https://www.nask.pl/magazyn/ai-w-e-administracji-publicznej-perspektywa-urzednikow-i-instytucji>
- Ministerstwo Cyfryzacji, Przewodnik po Sztucznej Inteligencji dla Administracji Publicznej, <https://ai.gov.pl/aktualnosci/przewodnik-dla-administracji-publicznej>
- Ministerstwo Cyfryzacji, Polityka Rozwoju AI w Polsce do 2030 roku, <https://ai.gov.pl/administracja-publiczna/polityka-rozwoju-ai>



Redakcja

## Socjotechnika. Jak działają cyberoszuści i jak chronić się przed zagrożeniem z ich strony?

W kontekście cyberbezpieczeństwa bardzo dużo mówi się o zabezpieczeniach z wykorzystaniem dedykowanej technologii. Ponadto, wiele miejsca zajmuje dyskusja na temat procedur, które mają chronić organizacje przed cyberzagrożeniami. Jednak obok tych dwóch aspektów, istotnym elementem przeciwdziałania hakerom jest budowanie świadomości wśród pracowników, jak również społeczeństwa. Wynika to z tego, że bardzo często oszuści zamiast łamać zabezpieczenia, decydują się „zaatakować” człowieka, który zaskoczony i pod presją staje się łatwiejszym celem aniżeli infrastruktura informatyczna. Dlatego, obok technologii i procedur, równie ważne w walce z oszustami internetowymi staje się budowanie świadomości społecznej na temat bezpieczeństwa. O tym w rozmowie z Podkomisarzem Wydziału do walki z Przestępczością Komputerową Komendy Miejskiej Policji w Rzeszowie.

Socjotechnika to jedna z metod manipulacji, stosowana przez oszustów internetowych w celu skłonienia grupy lub osoby do podjęcia ściśle określonych działań. W przypadku grupy zazwyczaj celem jest uzyskanie dostępu do systemów informatycznych, jeśli zaś chodzi o pojedynczą osobę, to wywierana na nią presja ma ją skłonić do przekazania pieniędzy. Niestety, pod presją i w strachu człowiek często traci czujność i reaguje pochopnie, co sprawia, że w ekosystemie cyberbezpieczeństwa to właśnie użytkownik końcowy często postrzegany jest jako najsłabsze ogniwo.

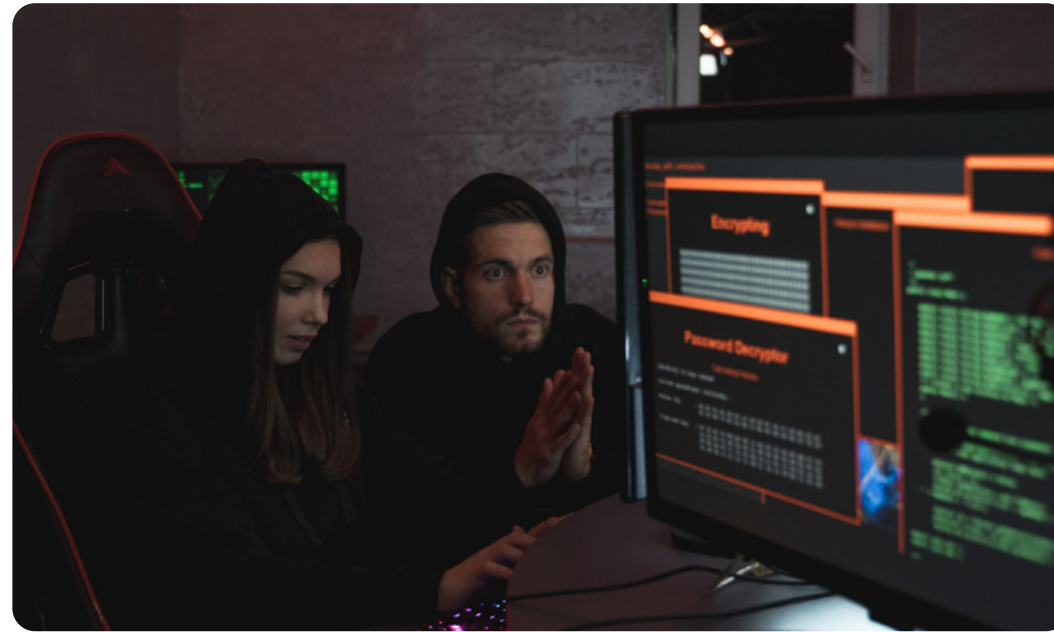
**Norbert Nowak:** Jednym z największych wyzwań cyberbezpieczeństwa jest minimalizacja ryzyk wynikających z zagrożeń skierowanych w użytkowników końcowego. Cyberprzestępcy doskonale wiedzą, że zamiast forsować zabezpieczenia techniczne, dużo lepiej w odpowiedni sposób „poprosić” nieświadomego użytkownika o dostęp do danych. Jak dziś wygląda skala oszustw socjotechnicznych, w których atakujący podszywają się pod urzędy i instytucje publiczne?

**Podkomisarz Przemysław Terlecki:** Zgodnie z prowadzonymi postępowaniami w Wydziale do walki z Przestępczo-

nością Komputerową Komendy Miejskiej Policji w Rzeszowie mogę powiedzieć, że oszustw związanych z podszywaniem się konkretnie pod urzędy lub instytucje publiczne nie ma zbyt wielu, jeżeli jednak już się pojawiają, mogą być bardzo dotkliwe. Co ciekawe najczęstszym modus operandi są przypadki tzw. oszustw „na policjanta” bądź „na prokuratora”, a więc wykorzystujące pewnego rodzaju respekt części społeczeństwa, w szczególności starszych osób, do organów ścigania, gdzie komunikacja następuje w najprostszym możliwym sposób, a więc poprzez połączenie telefoniczne.



Innym tego typu przypadkiem są akcje phishingowe realizowane drogą e-mail, gdzie sprawcy działają pod pretekstem popełnienia przestępstwa określonego w kodeksie karnym, często budzące go poczucie wstydu lub też wątpliwości „czy aby na pewno gdzieś nie kliknąłem”, jak na przykład pornografia dziecięca. W spreparowanym, często niedbale, piśmie cyberprzestępcy żądają dokonania opłaty na wskazany, na przykład zagraniczny numer bankowy, kontaktu e-mail z podaniem danych wrażliwych lub po prostu zawierających link, kod QR, w który chcą, aby ofiara weszła celem uniknię-



cia konsekwencji. Niestety może to powodować zainstalowanie na danym urządzeniu złośliwego oprogramowania typu Keylogger lub oprogramowania służącego na przykład do zdalnej obsługi pulpitu.

**Norbert Nowak:** Jakie schematy i techniki manipulacji są najczęściej wykorzystywane przez cyberprzestępców?

**Podkomisarz Przemysław Terlecki:** Schemat, jaki najczęściej pojawia się w naszej praktyce śledczej, to oszustwa inwestycyjne i bazowanie cyberprzestępców na dwóch elementach – niewiedzy jak funkcjonują kryptowaluty i chęci szybkiego wzbogacenia. W tym celu internetowi oszuści coraz częściej wykorzystują możliwości, jakie niesie za sobą sztuczna inteligencja. Na przykład przy oszustwach inwestycyjnych ludzie często wskazują, że na filmie reklamowym, który notabene był wyświetlany w mediach społecznościowych czy popularnych wyszukiwarkach, pojawiała się postać znanych publicznie osób. O ile młodsze pokolenia, wychowane już w dobie cyfrowej, poprzez jakość tego rodzaju filmów czy zdjęć pomijają je i odrzucają jako „deepfake”, to w przypadku osób starszych okazuje się to problematyczne, ponieważ wśród nich nowinki technologiczne nie są tak rozpoznawalne. Ponadto muszę wskazać tutaj na tworzenie presji czasu i poczu-

cia ekskluzywności. Prowadząc postępowania, często spotykałem się ze stwierdzeniami, że dana oferta obejmowała tylko i wyłącznie obywateli Polski, a przelew pokrzywdzony miał robić natychmiast, gdyż jakkolwiek zwłoka mogła prowadzić do konsekwencji skarbowych, karnych lub utraty wcześniej „zainwestowanych środków”. Konkludując, cyberprzestępcy bazują na deficycie wiedzy, chęci szybkiego zysku, pośpiechu i strachu.

**Norbert Nowak:** Z czego wynika skuteczność tego sposobu działania?

**Podkomisarz Przemysław Terlecki:** Z moich obserwacji wynika, że to ogólnospołeczny trend bazujący z jednej strony na pogoni za sukcesem, natomiast z drugiej na kreowaniu w mediach społecznościowych scenariuszy o tym, jak łatwo jest go osiągnąć. Przestępcy bezlitośnie to wykorzystują.

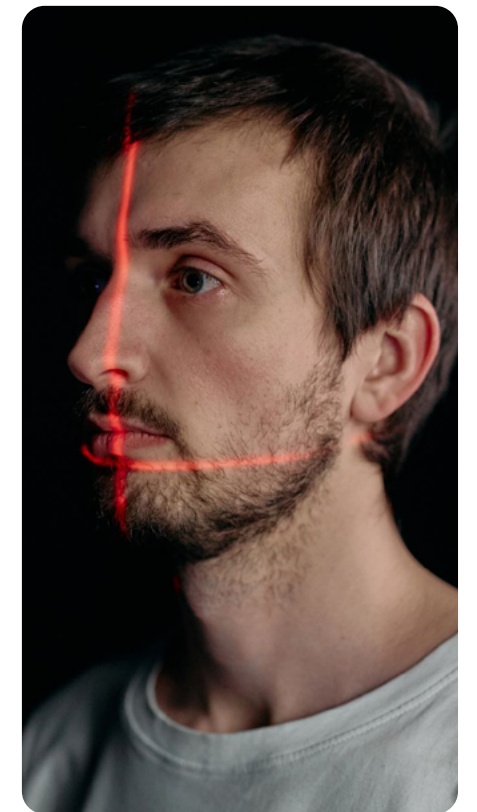
**Norbert Nowak:** Które grupy społeczne są dziś najbardziej narażone na takie zagrożenia i co sprawia, że to właśnie one stają się celem oszustów?

**Podkomisarz Przemysław Terlecki:** Przeważająca grupa przy oszustwach inwestycyjnych to osoby na emeryturze lub bliskie uzyskania praw emerytalnych, choć oczywiście zdarzają się wyjątki. Mianowicie osoby na początku swojej drogi zawodowej, które po rozpoczęciu wątpliwych inwestycji czy zaciągnięciu pożyczek, podjęły tak zwaną pracę dodatkową jako księgowy. Są to tzw. „muły finansowe”, czyli osoby które zakładają rachunki bankowe, przyjmują środki i kolejno w gotówce je wpłacają do bitomatów, gdzie środki te są już nie do odzyskania. Jeżeli weźmiemy pod uwagę, iż konkretna osoba nie posiada podstawowej wiedzy o funkcjonowaniu giełdy, a w szczególności giełdy kryptowalut, ma trudną sytuację materialną lub nie taką, jaką chciałaby mieć, to obietnica nagłej, diametralnej poprawy losu i zapewnienia dostatecznego życia sobie i najbliższemu sprawia, że emocje biorą górę nad racjonalną oceną sytuacji. Tym bardziej, że cyberprzestępcy, właśnie poprzez socjotechnikę, utwierdzają tę osobę w przekonaniu, że to właśnie dla niej przygotowana jest ta oferta. I dlatego najbardziej narażone są tutaj osoby starsze. Mają poczucie bycia w centrum uwagi rzekomych doradców

inwestycyjnych, którzy kreują przed nimi pasmo nieustających sukcesów.

**Norbert Nowak:** W jaki sposób nowoczesne technologie takie jak sztuczna inteligencja wpływają na sposób w jaki jesteśmy atakowani?

**Podkomisarz Przemysław Terlecki:** Dużo słyszymy w mediach o tzw. „deepfake’ach”, jednak to tylko wierzchołek góry lodowej, gdzie AI pozwala na masowe tworzenie materiałów wideo lub zdjęć. Jak wspominałem wyżej, przy oszustwach inwestycyjnych ludzie zachęceni są reklamami z wykorzystaniem wizerunków osób publicznie rozpoznawalnych, darzonych zaufaniem społecznym. Często w tym celu wykorzystywana jest sztuczna inteligencja, przez którą przestępcy modyfikują prawdziwą wypowiedź na taką, która nakłania do inwestycji. Z dotychczasowej praktyki mogę też nadmienić, że AI w tożsamy sposób wykorzystywana jest przy „oszustwach nigeryjskich”, określanych także jako romantyczne, gdzie albo wykorzystywany jest wizerunek aktorów, albo generowane są fikcyjne postacie, które swoją aparycją mają w pewien sposób przykuć uwa-



gę i uśpić czujność. W tym przypadku AI służy także do generowania wypowiedzi poprawnych językowo. Oczywiście do- tychczas skupiłem się na oszustwach inwestycyjnych, jednak mierzymy się także z szeregiem innych oszustw w cyberprze- strzeni, jak fałszywe sklepy internetowe, fałszywe oferty sprzedaży na platformach społecznościowych, oszustwa opierają- ce się na rzekomych opłatach za paczkę poprzez znanych przewoźników lub wy- łudzające dane bankowości elektronicz- nej, kart płatniczych pod pretekstem po- twierdzenia tożsamości dla odbioru środ- ków. Naprawdę, kreatywność cyberprze- stępców jest niemal nieograniczona i nie sposób odnieść się do każdego z przy- padków, a we wszystkim towarzyszy im właśnie sztuczna inteligencja.

**Norbert Nowak: Ofiary cyberataków i oszustw wirtualnych często nie mają świadomości na jaką pomoc mogą li- czyć ze strony służb. Wielu, stykając się z zagrożeniami nie wie czy i co mo- że zrobić. Jakie czynności w pierw- szej kolejności powinna podjąć osoba, która wykryje próbę wyłudzenia lub zostanie skutecznie zaatakowana?**

**Podkomisarz Przemysław Terlecki:** Naszą główną bronią, jako społeczeństwa, pozostaje ograniczone zaufanie, weryfi-



kacja każdej próby wyłudzenia danych wrażliwych czy środków finansowych. W przypadku próby cyberataków, oszustw internetowych, jako użytkowni- cy telefonów komórkowych musimy od- rzucić zaufanie do wyświetlanych na te- lefonie informacji i natychmiastowo prze- rwać rozmowę. Przestępcy stosują tzw. spoofing. Dla lepszego zobrazowania mo- dus operandi, przy oszustwie na pracow- nika banku początkowo oszuści posiadają szcztąkowe informacje jak imię, nazwisko, numer telefonu, na który dzwonią. W trak- cie rozmowy poprzez wzbudzanie poczu- cia zagrożenia, upływu czasu i konieczno- ści podjęcia natychmiastowych działań, zdobywają informację na temat naszego banku, po czym rozłączają się. Następ- nie otrzymujemy połączenie, które telefon poprzez sieć komórkową przypisuje do połączenia z banku. Natomiast potencjal- ny pokrzywdzony, aby uchronić się przed oszustwem, sam powinien wybrać numer do swojego banku, zadzwonić do swo- jej rodziny z informacją o tej sytuacji lub po prostu udać się do placówki danego podmiotu. Niestety, zdecydowana więk- szość ludzi bezkrytycznie ulega przed- stawionej legendzie, jaką budują spraw- cy i nawet idąc do placówki banku mniej ufają pracownikowi, rzeczywistej osobie niż tej, która kieruje jej zachowaniem ze słuchawki telefonu. Jeżeli już osoba pad- nie ofiarą cyberoszustwa, to musi mieć

świadomość, że liczy się sprawne pod- jęcie działań przez Policję i banki. W tym celu zawiadamiający musi mieć dane, wy- druk przelewu, wygenerowane potwier- dzenie w telefonie, co pozwoli na zwró- cenie się o blokadę środków za pośred- nictwem dostępnych narzędzi. Inaczej sy- tuacja przedstawia się przy umożliwieniu sprawcom zbudowania wirtualnej infra- struktury przez dłuższy czas, kiedy da- ne pokrzywdzonego mogły już posłużyć do utworzenia innych kont bankowych i wyprowadzeniu środków finansowych na przykład w kryptowaluty. Wtedy naj- ważniejsze jest zgromadzenie całości da- nych w postaci numerów telefonów, ad- resów e-mail, numerów rachunków ban- kowych, które wynikają z dokonywanych przelewów, adresów portfeli kryptowalut.

**Norbert Nowak: Gdzie w takiej sytu- acji można się zgłosić po pomoc i w jakich sytuacjach takie wsparcie jest dostępne?**

**Podkomisarz Przemysław Terlecki:** Po pierwsze bank, który ma swoje moż- liwości do blokowania przepływu środ- ków finansowych. Jednak pracownicy od- powiednich departamentów muszą uzy- skać informację natychmiast po zdarze- niu, dlatego osoba samodzielnie musi wy- brać numer do swojego banku i zabloko- wać bankowość elektroniczną, złożyć re- klamację. Warto pamiętać, że cyberprze- stępcy wykorzystują najsłabszy element infrastruktury bankowości, czyli człowie- ka. Podanie hasła, loginów, akceptacja przelewu, generowanie kodów BLIK, nawet



w przypadku działania w błędzie nie prze- rzuca odpowiedzialności na bank. Kolej- nym krokiem jest powiadomienie najbliż- szych o zdarzeniu, od których osoba mo- że uzyskać pomoc, wsparcie. Jest to o ty- le istotne, że w przypadku przełamań za- bezpieczeń do platform społeczności- wych i pojawienia się wśród najczęst- szych kontaktów próśb o kod BLIK, to naj- bliżsi mogą stracić swoje środki finanso- we i nawet najprostszy post ostrzegający o takiej sytuacji może zapobiec utracie przez nich pieniędzy. Ostatnim krokiem jest złożenie zawiadomienia do organów ścigania. I tutaj najistotniejsze jest zgro- madzenie danych, które w ramach postę- powania mogą zostać wykorzystane do podjęcia czynności dowodowych. Z uwa- gi na ilość rodzajów cyberprzestępstw nie ma tak naprawdę idealnego scenariusza postępowania dla osób pokrzywdzonych. Dlatego nadmienię jeszcze, że w przypad- ku, gdy osoba prowadzi działalność gos- podarczą i cyberprzestępcy podszy- wają się pod jej markę, warto też zwró- cić się do CERT Polska poprzez zgłosze- nie incydentu na stronie [www.incident.cert.pl](http://www.incident.cert.pl). Ta instytucja zajmuje się między innymi blokowaniem fałszywych domen i analizą zagrożeń w polskim Internecie.



**Norbert Nowak: Jaką rolę odgrywa policja w procesie minimalizacji skut- ków cyberataków? Jakie konkretne zadania realizuje?**

**Podkomisarz Przemysław Terlecki:** Po- licja, jako organ ścigania, w celu minimali- zacji skutków cyberataków działa na wie- lu płaszczyznach. Przy przyjęciu zawi- adomienia funkcjonariusze pionu docho- dzeniowo-śledczego podejmują działa- nia blokowania przepływów finansowych, oczywiście jeżeli modus operandi spraw- ców bazuje na przelewach międzybanko- wych. Kolejno, już na etapie prowadzenia postępowania przygotowawczego funk- cjonariusz zajmuje się ustalaniem, a na- stępnie zabezpieczaniem dowodów cy- frowych. W przypadku, gdy zgromadzony materiał dowodowy uzasadnia taką ko- nieczność, to w wyniku funkcjonujących umów międzynarodowych we współpra- cy z Prokuraturą Policja podejmuje czyn- ności śledcze w ramach Międzynarodo- wych Pomocy Prawnych lub Europejskich Nakazów Dochodzeniowych. Użytkowni- cy sieci Internet, a tym samym poten- cjalne ofiary cyberataków muszą pamię- tać o tym, że Internet, w przeciwieństwie do systemów prawnych, nie respektuje państwowych granic. Końcowym eta- pem jest ustalenie sprawców i przygo- towanie materiału dowodowego skutku- jącego skierowaniem do Sądu aktu oskar- żenia. Niewątpliwie, w wyniku możliwości jakie oferują nowoczesne narzędzia, jest to najtrudniejszy etap naszych działań.

**Norbert Nowak: Mówi się, że najlepiej zapobiegać. Jakie więc działania pre- wencyjne podejmuje policja w celu ograniczenia działalności cyberprze- stępców?**

**Podkomisarz Przemysław Terlecki:** Działania prewencyjne podejmowane przez Policję to przede wszystkim eduka- cja, akcje ostrzegawcze, działalność pra- sowa, kampanie informacyjne oparte na aktualnych trendach. Do tego typu dzia- łań są wyznaczone komórki, które orga- nizują prelekcje, spotkania w szkołach, ale także zamieszczają artykuły w serwisach Internetowych, których zadaniem jest po- szerzanie świadomości o modus operandi cyberprzestępców. Podsumowując, nasza prewencja to kolokwialnie mówiąc, ciągły wyścig zbrojeń. Staramy się być o krok przed przestępcami i zamienia- my wiedzę zdobytą w toku postępowań przygotowawczych na praktyczne rady, które mogą przyczynić się do poszerza- nia świadomości i mieć realny wpływ na przeciwdziałanie cyberprzestępczości.

**Norbert Nowak: Szerokie wyko- rzystanie technologii w życiu co- dziennym zwiększa ryzyka związane z oszustwami w warstwie wirtualnej. Budowanie świadomości społecznej w tym zakresie to jedno z istotnych zadań samorządów, dbających o swo- ich mieszkańców. W jaki sposób wła- dze lokalne mogą pomóc w budowa- niu kultury cyberbezpieczeństwa**

### w swoich społecznościach?

**Podkomisarz Przemysław Terlecki:** Samorząd jest naturalnym partnerem Policji, ponieważ ma coś, czego służby często szukają – bezpośrednie i codzienne kanały dotarcia do mieszkańców. Samorządy w ramach swojej działalności odpowiadają za szkoły, jednostki samorządowe, koła gospodyń wiejskich i inne, jak domy kultury, biblioteki publiczne. Ich głównym atutem w budowaniu kultury cyberbezpieczeństwa jest więc rozbudowana infrastruktura społeczna. W ramach działalności tychże struktur samorządy mogą budować świadomość społeczeństwa w jaki sposób działają cyberprzestępcy. Zgodnie z moją wiedzą funkcjonują w wielu miastach Uniwersytety Trzeciego Wieku, a jak wspominałem osoby starsze to największa grupa osób zagrożonych cyberprzestępczością. Ponadto istotne jest też informowanie o zdarzeniach, które już się wydarzyły za pomocą środków masowego przekazu, profili społecznościowych urzędów lub gazetach samorządowych. Mieszkańcy powinni mieć świadomość,



że cyberprzestępczość to nie abstrakcyjne pojęcie, ale element codziennego życia ludzi. Kluczowe jest osvajanie z technologią w sposób bezpieczny – pokazywanie, że „konsultant” z ekranu czy słuchawki nie zawsze ma dobre zamiary.

**Norbert Nowak: Co z perspektywy służb najbardziej zwiększyłoby odporność społeczną na tego typu zagrożenia?**

**Podkomisarz Przemysław Terlecki:** Edukacja, zarówno szkolna w ramach zajęć z informatyki, godzin wychowawczych, jak i wspomniana wcześniej praca z osobami starszymi w ramach działalności jednostek samorządu terytorialnego. Nie można też pominąć zainteresowania funkcjonowaniem osób starszych przez ich rodziny. Jeżeli widzimy, że nasi seniorzy nagle spędzają więcej czasu przy telefonach, w celu rozmowy telefonicznej wychodzą do innego pokoju, zaczynają użytkować komputer w trakcie rozmowy telefonicznej warto jest sprawdzić i podpytać, z czego to wynika. Czy wszystko u nich dobrze lub wprost zapytać o to, czy nie natrafiły w sieci na intratne oferty inwestycyjne i doradców mówiących w języku polskim, ale wyraźnie słyszalnym wschodnim akcentem. Osobiście w niektórych postępowaniach, rozmawiając z pokrzywdzonymi, słyszałem o tym, że teraz wstydzą się powiedzieć,

co zrobili i nie chcą zwracać komuś głowy. Niestety, ale to może wynikać z braku odpowiedniego poziomu zainteresowania osobami starszymi. Jeżeli chodzi o najmłodszych, to ważny jest nadzór i weryfikacja ich aktywności w sieci Internet, na przykład ustawione limity płatności czy dwustopniowa weryfikacja (2FA) wydatków w abonencie telefonicznym, koncie Google Pay i innych tego typu mechanizmach płatniczych.



**Norbert Nowak: Czy i jak samorządy mogą współpracować z policją, aby skuteczniej docierać do mieszkańców?**

**Podkomisarz Przemysław Terlecki:** Współpraca na linii Policja-Samorząd to jeden z najskuteczniejszych sposobów na dotarcie do mieszkańców z profilaktyką tam, gdzie jest ona najbardziej potrzebna. Widzimy tu ogromny potencjał, szczególnie w inicjowaniu programów edukacyjnych wykraczających poza standardową podstawę programową. Cyberbezpieczeństwo powinno być stałym elementem edukacji nie tylko dla uczniów, ale i dla rodziców, dziadków, osób starszych, którzy często nie są świadomi zagrożeń. W tym zakresie Policja zawsze jest otwarta na współpracę. Osobiście brałem udział w spotkaniu z uczniami jednej z rzeszowskich szkół na temat oszustw internetowych i „deepfake’ów”. Wiem, że Strzelnica Powiatu Rzeszowskiego planuje w ramach współpracy z Komendą Miejską Policji w Rzeszowie organizację szerszych zajęć edukacyjno-obronnych, w których planowane są bloki tematyczne poświęcone właśnie cyberbezpieczeństwu. Samorząd ma infrastrukturę, my mamy wiedzę ekspercką – połączenie tych sił to najlepsza tarcza dla naszych mieszkańców. Na koniec pozwolę sobie nadmienić, że w świecie cyberprzestępstw głównym elementem jest podszywanie się. I tu powrócę do pierwszego pytania, nie musi być to urząd, policjant, prokurator. Oszuści podszywają się pod sprzedawców na platformach sprzedażowych, tworząc sprepara-

wane strony internetowe, gdzie do odebrania płatności konieczne jest podanie danych karty płatniczej, które w rzeczywistości umożliwiają przestępcom dokonywanie płatności w sieci Internet. Kolejno podszywają się pod pracowników firm przewozowych do podania danych osobowych i bankowych do rzekomego odbioru płatności, co znowu umożliwia im dostęp do bankowości elektronicznej pokrzywdzonego. Jak wspominałem wcześniej, kreatywność cyberprzestępców jest nieograniczona, ale nie dotyczy tylko oszustw na zatrważające kwoty, są to też drobne przestępstwa przy sprzedaży przedmiotów na platformach społecznościowych. Tu też dochodzi do podszywania się sprawców pod osobę, która albo nie jest świadoma przejęcia jej konta społecznościowego, albo w rzeczywistości nie istnieje, a wszystko zostało wygenerowane przez sztuczną inteligencję.

**Norbert Nowak:** Jak więc widać, cyberbezpieczeństwo dotyczy każdego – nie tylko podmiotów gospodarczych, ale również osób prywatnych, które na co dzień korzystają z telefonów komórkowych, e-usług publicznych czy płatności online. Dlatego tak ważne staje się ciągłe edukowanie na temat cyfrowych zagrożeń, w które na równi powinny być zaangażowane służby i samorząd – pozwala to dotrzeć z informacją do każdej z grup narażonych na działania oszustów. Dziękuję za rozmowę i pamiętajmy, że świadomość, zasada ograniczonego zaufania i wzmożona czujność to proste, a zarazem najlepsze sposoby obrony przed manipulacją.

### Podkomisarz Przemysław Terlecki

**Wydział dw. z Przestępczością Komputerową KMP Rzeszów**

Służbę w Policji rozpoczął w 2015 roku w Oddziale Prewencji Policji w Krakowie. Od 2020 roku jest funkcjonariuszem Komendy Miejskiej Policji w Rzeszowie, gdzie pełnił służbę w Wydziale do walki z Przestępczością Gospodarczą. Od końca 2025 roku działa w strukturach Wydziału do walki z Przestępczością Komputerową.



### Norbert Nowak

Ekspert cyberbezpieczeństwa. Zajmuje się realizacją usług związanych z analizą i projektowaniem infrastruktur pod kątem ochrony systemów i danych. Zrealizował liczne projekty w zakresie networkingu, storage’u, wirtualizacji oraz bezpieczeństwa IT. Prelegent i panelista konferencji branżowych, a także autor publikacji dziedzinowych.

## Opinie ekspertów

### Jak wiedza i doświadczenie administratorów IT w urzędach wpływają na bezpieczeństwo całej jednostki i realizację wymagań Krajowego Systemu Cyberbezpieczeństwa? W jaki sposób skutecznie rozwijać ich kompetencje?



Administrator IT w urzędzie nie jest już „osobą od komputerów”, lecz operatorem ciągłości usług publicznych. To jego wiedza decyduje, czy wymagania NIS2/KSC2 zostaną przełożone z dokumentacji SZBI na zabezpieczenia: inwentaryzację aktywów, aktualizacje oparte na ryzyku, uprawnienia i poprawnie wdrożone MFA, segmentację sieci, centralne logowanie i monitoring, odseparowane kopie zapasowe oraz regularne testy odtworzenia. Doświadczony administrator szybciej rozpozna anomalie, ograniczy zasięg incydentu i zachowa materiał dowodowy; niedobór kompetencji tworzy natomiast „ślepe strefy”, w których jedna błędna konfiguracja może zatrzymać urząd i usługi dla mieszkańców.

Od 3 kwietnia 2026 r. KSC przypisuje odpowiedzialność kierownikowi jednostki także po delegowaniu zadań i wymaga jego corocznego szkolenia. Administrator musi więc otrzymać nie tylko obowiązki, ale także budżet, czas, uprawnienia do podejmowania decyzji i zastępstwo na czas nieobecności. Kompetencje nale-

ży rozwijać praktycznie: poprzez łączenie potrzebnych umiejętności z potencjalnym ryzykiem, praktyczne laboratoria, scenariusze ransomware i awarii, testowe odtwarzanie kopii, symulację zgłoszeń w terminach 24/72 godzin oraz analizę incydentów. Certyfikat przy takiej nauce jest dodatkiem, nie celem. Miara dojrzałości powinny być czas wykrycia i reakcji, pokrycie MFA w organizacji, tempo łatania podatności i skuteczność odtworzeń z kopii. KSC nie wdraża się segregatorem – wdraża się konfiguracją, logami i przeciwczytnym działaniem, które we wspomnianych segregatorach są skrupulatnie opisane.



**Maciej Szymczak**

CISO, Securitem Szkolenia

### Jakie są najczęstsze wyzwania przy wdrażaniu samoobsługi pracowniczej w sektorze publicznym w związku ze złożonością obowiązujących procedur?



W ostatnich latach obserwujemy w sektorze publicznym rosnącą świadomość potrzeby upraszczania procesów. Choć złożoność procedur nadal jest naturalną cechą wielu organizacji publicznych, coraz częściej kierownictwo jednostek dostrzega nadmierną liczbę kroków, wąskie gardła oraz czynności, które nie wnoszą wartości do procesu. W efekcie projekty wdrożeniowe coraz częściej rozpoczynają się od wspólnego przeglądu i optymalizacji procesów, a nie wyłącznie od ich odwzorowania w systemie. Klienci oczekują dziś nie tylko technologii, ale również wsparcia doradczego w zakresie usprawniania organizacji pracy. W praktyce największe korzyści osiągają te organizacje, które traktują wdrożenie samoobsługi pracowniczej jako okazję do przeglądu i uproszczenia procesów, a nie jedynie do przeniesienia istniejących formularzy i procedur do wersji elektronicznej.

Bardzo ważną okazuje się również związana z cyfryzacją samoobsługi zmiana organizacyjna, czyli zmiana dotychczasowego sposobu pracy – tak po stro-

nie specjalistów HR, jak i pracowników organizacji. Kluczowa staje się tu intuicyjność wdrażanych narzędzi, która ułatwi użytkownikom stopniowe korzystanie z nowych funkcjonalności, a także wsparcie merytoryczne w postaci warsztatów lub szkoleń.

Na sukces wdrożenia składa się więc kilka czynników. Wybór i połączenie technologii z uporządkowaniem procesów oraz zarządzaniem zmianą w organizacji. Odpowiednio dobrane i skonfigurowane rozwiązania, jak Teta HR i Teta ME, pozwalają nie tylko odwzorować złożone procedury, ale również realnie je usprawnić w zgodzie z aktualnymi przepisami i standardami bezpieczeństwa.



**Krzysztof Sołowski**

Solution Consulting Manager,  
Unit4 Polska

### Na jakich obszarach powinny skupiać się JST w pierwszej kolejności, aby uzyskać największy efekt w zakresie bezpieczeństwa przy ograniczonych budżetach?



Bezpieczeństwo infrastruktury w JST jest zagadnieniem ważnym, jednak przy mniejszych działach IT i ograniczonych budżetach może wymagać kompromisów. Wówczas ważne staje się ustalenie odpowiednich priorytetów i określenie ryzyk o wysokim prawdopodobieństwie, których ograniczenie można osiągnąć niewielkim kosztem. W mniejszych organizacjach punktem wyjścia powinna być ochrona tożsamości i dostępu, w czym pomoże uwierzytelnianie wieloskładnikowe (AD SelfService). Już samo zabezpieczenie kont użytkowników, poczty email czy systemów zdalnego dostępu zmniejsza ryzyko przejęcia konta i utraty danych. Kolejną kwestią jest kontrola uprawnień, obejmująca regularne audyty dostępu i AD Audit, która pozwala na bieżąco weryfikować i szybko odbierać zbędne uprawnienia. Na koniec zarządzanie podatnościami, czyli regularne aktualizowanie oprogramowania stacji roboczych, serwerów i aplikacji celem eliminowania luk w zabezpieczeniach oraz błędnych konfiguracji. Jak więc widać, nawet bez wielu kosztownych narzędzi, a za pomocą właściwych działań można znacząco ograniczyć powierzchnię ataku.

Nieco inne podejście będzie potrzebne w większych JST, zwłaszcza obsługujących wiele podmiotów podległych. Tutaj pomocne stanie się centralne monitorowanie i zarządzanie całością tego rozproszonego środowiska. Mowa o Endpoint Central do zarządzania urządzeniami końcowymi (UEM), zapewniającymi administratorom IT widoczność i możliwość zdalnego wykonywania działań, wsparcia użytkowników i uruchamiania zabezpieczeń typu antymalware, EDR, zapobiegania wyciekom danych, itd. Warto też rozważyć zarządzanie zgłoszeniami i incydentami oraz zidentyfikowanymi ryzykami. Kolejnym obszarem może być wprowadzenie narzędzi klasy LOG360 do monitorowania zdarzeń i wykrywania zagrożeń, wraz z odpowiednimi automatyzacjami, jak i PAM360 do zarządzania kontami uprzywilejowanymi i dostęпами dla kontraktorów.



**Dominik Ciszewski**

Channel Account Manager w MWT  
Solutions, dystrybutor ManageEngine

# KONFERENCJA CyberSanta

## by OPTeam vol.3

- AI kontra cyberzagrożenia
- Cyberodporność w praktyce
- NIS2 i KSC bez tajemnic

**Zapraszamy na wydarzenie**

<https://opteam.pl/wydarzenia/cybersanta-by-opteam-vol3-35.html>

**OPTeam**  
EKSPERT ROZWIĄZAŃ IT

**Data:**  
**3 grudnia 2026**

**Miejsce:**  
**Apart Hotel 12, Rzeszów**

## ■ Krótki komentarz

# Multiportal zmienia logikę cyfryzacji jednostek samorządu terytorialnego

Wraz z cyfrowym rozwojem administracji publicznej przybywa nie tylko portali służących do zarządzania informacją, ale również aplikacji webowych, których celem jest udostępnienie e-usług społeczności lokalnej. Rosnąca liczba często niezależnych rozwiązań, obsługiwanych z poziomu różnych technologii, zwiększa złożoność i koszty środowiska. Alternatywą dla nadmiaru i rozproszenia jest multiportal, z którym samorząd może uporządkować obecny stan, rozwijając komunikację i współpracę cyfrową bez technologicznego chaosu.



Największą zaletą wdrożenia multiportalu jest zdolność uporządkowania ekosystemu rozwiązań JST – serwisów, aplikacji, e-usług, co pomaga ograniczyć koszt utrzymania środowiska z zachowaniem swobody jego rozwoju.

Centralne środowisko multiportalowe nie obejmuje wyłącznie rozwiązań danej JST. Obok portali i aplikacji urzędu miasta czy gminy z powodzeniem można w nim utrzymywać serwisy szkół, przedszkoli, ośrodków kultury czy bibliotek. Zamiast inwestować w odrębne technologie dla każdego rozwiązania, wystarczy wdrożyć jeden multiportal, który pozwala na współdzielenie funkcjonalności i globalne zarządzanie treścią, rolami i uprawnieniami, a także integrację z innymi systemami.

## 5 najważniejszych korzyści

### 1. Niższe koszty w całym cyklu życia rozwiązań.

Inwestycja w jedno środowisko, na którym można budować kolejne portale, aplikacje i cyfrowe usługi, to w praktyce mniejszy koszt zarządzania cyklem życia rozwiązań. Eliminuje wydatki związane z zakupem kolejnej technologii, jej wdrożeniem i konfiguracją funkcjonalności, a w perspektywie aktualizacją i rozwojem. Uruchomienie nowego rozwiązania zajmuje zdecydowanie mniej czasu i wymaga mniej pracy.

### 2. Jeden system zamiast rozproszonych technologii.

W przypadku organizacji posiadających wiele jednostek, a tym samym zespołów odpowiedzialnych za publikację informacji, zaletą wykorzystania multiportalu będzie centralizacja zarządzania treścią. Nie oznacza to jednak, że jedna osoba odpowiada za wszystkie istniejące projekty. Administrator może przyznać dostęp ze względu na domenę i rolę, z dokładnym określonym zakresem uprawnień. Do tego jedna baza danych sprzyja spójności komunikacyjnej, eliminując problem wielokrotnego wprowadzania czy aktualizowania treści w różnych systemach.

### 3. Szybsze uruchamianie nowych rozwiązań.

Z platformą multiportalową nie trzeba od podstaw budować cyfrowego środowiska za każdym razem, gdy zachodzi konieczność uruchomienia nowego projektu. W ramach jednej inwestycji JST zyskuje bazę technologiczną do nowych inicjatyw wynikających czy to z potrzeb lokalnych, czy też ogólnych dyrektyw w sektorze publicznym.

### 4. Rozwój z zachowaniem dyscypliny finansowej.

W związku z rosnącym zakresem cyfrowych usług JST szczególnego znaczenia nabiera skalowalność platformy multiportalowej. Dzięki niej architektura cyfrowego samorządu może być stopniowo rozbudowywana o nowe rozwiązania, a samo środowisko pozostanie wydajne bez względu na liczbę uruchomionych projektów.

### 5. Jeden standard dostępnych cyfrowo rozwiązań.

Istotnym zagadnieniem zarządczym jest utrzymanie wspólnego standardu dostępności cyfrowej posiadanych portali, aplikacji i e-usług. W jednym środowisku multiportalowym staje się to łatwiejsze, oczywiście pod warunkiem, że obsługuje ono obowiązujący standard WCAG.

Multiportal to inwestycja w uporządkowaną architekturę cyfrową samorządu. Nie tylko rozwiązuje problem dużej liczby rozproszonych rozwiązań, ale w miarę postępującej cyfryzacji pomaga wdrażać i rozwijać kolejne narzędzia bez kosztownych wdrożeń czy modyfikacji.



**Maciej Stanisławczyk**

Ekspert do spraw nowych technologii. Dzięki wiedzy na temat sektora publicznego i analizie trendów doradza w zakresie doboru rozwiązań wpisujących się w cyfrowe potrzeby instytucji i spełniających wymogi prawne rynku.

# Platforma cyfrowej komunikacji dla JST

Jeden ekosystem dla wszystkich portali, aplikacji i e-usług.



## Wygoda

Wszystkie rozwiązania internetowe w jednym spójnym miejscu.



## Funkcjonalność

Centralne środowisko rozwijające się razem z potrzebami JST.



## Bezpieczeństwo

Poprawa poziomu cyberbezpieczeństwa dzięki ograniczeniu technologii.

**Mniejsze rozproszenie, większa kontrola. Multiportal to gotowość na kolejne etapy cyfryzacji.**



**Zeskanuj kod i dowiedz się więcej**



# CYFROWY SEKTOR PUBLICZNY

<http://opteam.pl/biuletyn>



---

Wydawca:

**OPTeam**  
EKSPERT ROZWIĄZAŃ IT

36-002 Jasionka  
Tajęcina 113

tel. 17 867 21 00  
email: [opteam@opteam.pl](mailto:opteam@opteam.pl)

NIP: 813-03-34-531  
REGON: 008033000  
KRS: 0000160492OPTeam S.A.

2026 OPTeam SA  
Wszelkie prawa zastrzeżone.