2/2026

CYFROWY SEKTOR PUBLICZNY

Praktyczne rozwiązania i kierunki rozwoju

JAK EFEKTYWNIE I Z ZYSKIEM ZARZĄDZAĆ OBIEKTAMI SPORTOWO-REKREACYJNYMI?

Temat wydania

CYBERBEZPIECZEŃSTWO W CENTRUM UWAGI. RELACJA Z CYBERSUMMIT PODKARPACIE 2026

Materiały konferencyjne

BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH W KONTEKŚCIE ROZWIĄZAŃ HOSTINGOWYCH

Artykuł praktyczny

CYFROWE USŁUGI PUBLICZNE W PRAKTYCE. OD REGULACJI PRAWNYCH DO REALNEJ WARTOŚCI DLA URZĘDU I MIESZKAŃCA

Krótki komentarz

Cykl

W minutę o... rozwiązaniach dla sektora publicznego

OBEJRZYJ

01. Jak chatbot AI zwiększa dostępność JST w komunikacji z mieszkańcami?

02. Jak AI pomaga sprostać wymogom WCAG 2.2 w tworzeniu serwisów internetowych?

03. Jak ograniczyć konieczność inwestowania w wiele systemów CMS?

04. Jak efektywnie i z zyskiem zarządzać obiektami sportowo-rekreacyjnymi?

05. Jak ograniczyć czas obsługi informacyjnej pracowników przez dział HR?

Zeskanuj kod i obejrzyj

Bądź na bieżąco

https://www.youtube.com/@OPTeamSA

Spis treści

Tematy wydania

Jak reagować na incydenty? Standardy właściwej obsługi zdarzeń w środowisku IT

Skuteczny system bezpieczeństwa nie powinien dzisiaj unikać ataków, a potrafić je odpierać.

Artykuł praktyczny

WCAG 2.2. Nowy standard dostępności cyfrowej portali jednostek sektora publicznego

WCAG to nie tylko zestaw wytycznych technicznych, ale też standard jakości usług cyfrowych.

Redakcja

Krzysztof Pliś
Bartosz Balawender
Bogumiła Szwedo
Magdalena Tobiasz
Aleksandra Stachowicz

Jak efektywnie i z zyskiem zarządzać obiektami sportowo-rekreacyjnymi?

Przeprowadzone w ostatnich latach kontrole NIK wykazały, że jednostki administracji publicznej nie zawsze efektywnie wykorzystują potencjał obiektów sportowo-rekreacyjnych na swoim terenie. Dotyczy to na równi tych większych, jak i mniejszych typu Orliki, sale gimnastyczne czy boiska szkolne. Trudności w zarządzaniu nimi po części wynikają z braku kompetencji w tej dziedzinie, a po części z braku narzędzi wspomagających tę procedurę. Tymczasem istnieje do tego skuteczne, dedykowane rozwiązanie.

Popularyzacja aktywności fizycznej przyczyniła się do wzrostu ilości atrakcyjnych obiektów sportowych i rekreacyjnych. Powstało wiele nowych, a już istniejące zostały zmodernizowane. Jednak mimo tego, obiekty te wciąż nie są częściej aniżeli wcześniej użytkowane, mimo że społeczeństwo zdaje się wykazywać nimi coraz większe zainteresowanie. Przyczyn takiego stanu rzeczy jest kilka, a każdą z nich w większym lub mniejszym stopniu można wyeliminować przy wsparciu nowych technologii.

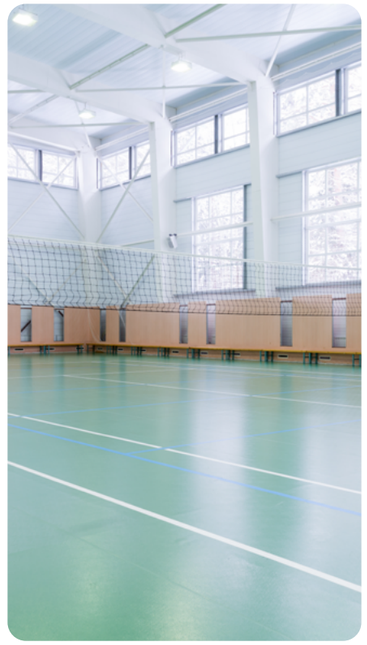
Dostępność informacji o infrastrukturze

Najczęstszym problemem związanym z zarządzaniem obiektami sportowymi jest brak łatwo dostępnej informacji o nich dla mieszkańców, którzy nie zawsze wiedzą o istnieniu w ich regionie tej infrastruktury, o możliwości jej komercyjnego wynajmu, ani o zasadach na jakich się to odbywa. W związku z tym naturalnym jest, że nie podejmują inicjatywy w celu skorzystania z niej i w zdecydowanej większości przypadków pozostaje ona mało lub wcale nie użytkowana. Tak więc, brak informacji, rozumianej jako promocja obiektów i możliwości ich wynajmu, przekłada się na małe zainteresowanie i znikome użytkowanie, co w konsekwencji może powodować straty, podczas gdy ośrodki sportowe czy sale gimnastyczne z powodzeniem mogą przynosić wymierne zyski, a nawet stać się dodatkowym źródłem renowacyjnych inwestycji.

> **Ośrodki sportowe czy sale gimnastyczne mogą przynosić zyski i stać się źródłem renowacyjnych inwestycji.**

Kolejna kwestia to brak bieżących informacji na temat obłożenia obiektów sportowych dla osób administrujących i jednostek nadrzędnych. O ile jeszcze mają oni wiedzę o eksploatacji ośrodków sportowo-rekreacyjnych, o tyle w większości przypadków nie posiadają statystyk na temat stopnia obłożenia i użycia hal sportowych, sal gimnastycznych, boisk szkolnych czy Orlików. Z tego powodu bardzo trudno jest ocenić tendencje odnośnie stopnia zainteresowania nimi i chęci ich wynajmu w celach komercyjnych. Nie widać, gdzie tkwi potencjał, a gdzie wymagana jest zmiana podejścia.

Istotna okazuje się również transparentność i wygoda procedury wynajmu obiektu. Zazwyczaj związane jest to z koniecznością kontaktu telefonicznego z zarządzającym nim administratorem, a często wymaga też osobistej wizyty w celu pozyskania informacji na temat zasad udostępniania i związanych z tym procedur. Również kwestie formalne muszą być dopełniane osobiście i w sposób manualny, co dla wielu osób może stanowić utrudnienie i okazać się zniechęcające szczególnie w czasach, kiedy to wiele spraw można dopełnić online.



Tak więc, podstawą efektywnego zarządzania okazują się dostępność informacji na temat istniejącej infrastruktury, dobra promocja obiektów tych większych i mniejszych, cyfryzacja usługi wynajmu – ułatwiająca administrowanie i zarządzanie oraz dopełnianie formalności, a także statystyki dotyczące eksploatacji, które odzwierciedlają potencjał obiektów oraz tendencje związane z użytkowaniem.

> **Efektywne zarządzanie obiektami sportowo-rekreacyjnymi to dostępność informacji, dobra promocja, cyfryzacja usługi wynajmu i statystyki dotyczące eksploatacji.**

Budowa kompetencji zarządzania obiektami

Zarządzanie obiektami sportowymi i rekreacyjnymi wymaga wypracowania kompetencji i metod o charakterze biznesowym. Dlatego w wielu przypadkach ten obszar działalności statutowej jednostek samorządowych jest komercjalizowany, a obowiązki w tym zakresie delegowane są na spółki świadczące usługi menadżerskie. I choć takie podejście jest dużym ułatwieniem, to jednak wiąże się z pewnym kosztem, który dla budżetu może stanowić dodatkowe obciążenie. Co więcej, outsourcing rozpatrywany jest głównie w kontekście dużych obiektów, podczas gdy na terenie miasta i gminy funkcjonuje ich o wiele więcej, w tym dużo mniejszych. I te choć podlegają jednostkom samorządu, są niezależnie i we własnym zakresie administrowane. Przykładem są choćby sale gimnastyczne czy boiska w szkołach, którymi w zakresie dostępności zarządzają dyrektorzy placówek.

> **Technologia może stać się podstawą promocji i wynajmu, a dzięki wskaźnikom efektywności również elementem zarządzania cyklem życia infrastruktury sportowo-rekreacyjnej.**

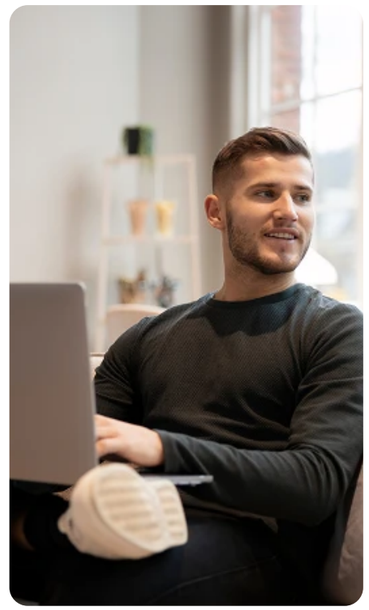
Stąd też korzystniejszym podejściem jest budowa kompetencji menadżerskich we własnym zakresie, co jednak wymaga czasu i zaangażowania w budowę modelu wykorzystania infrastruktury oraz jej skutecznej promocji – w obu przypadkach konieczna jest forma dostosowana do lokalnej społeczności. Do tego z kolei potrzebna jest interdyscyplinarna wiedza, jak znajomość marketingu, finansów, zarządzania czy prawa – m. in. w zakresie bezpieczeństwa czy odpowiedzialności zarządczej, co rzadko rozwijane jest poprzez szkolenia czy ścieżki specjalizacji zawodowej, a częściej stanowi umiejętności nabyte. Jednostki samorządu terytorialnego nie zawsze też dysponują zasobami kadrowymi do profesjonalnego zarządzania infrastrukturą sportową. W praktyce więc wielu zarządzających obiektami w JST pełni rolę administratorów technicznych, a nie menedżerów rozwijających ofertę.

W rezultacie wyzwania kompetencyjne przekładają się na niską efektywność ekonomiczną obiektów.

Tymczasem ułatwieniem okazuje się technologia, która może stać się nie tylko podstawą promocji i wynajmu, ale również elementem zarządzania cyklem życia infrastruktury, gdzie łatwo dostępne statystyki efektywności mogą być pomocne w planowaniu utrzymania i modernizacji.

Narzędzie wspierające administrowanie i raportowanie

Rozwiązaniem wspierającym zarządzanie obiektami sportowymi różnej wielkości jest System Obsługi Rezerwacji Obiektów Sportowych, który powstał z myślą zarówno o osobach zarządzających miastami, gminami oraz starostwami, jak i bezpośrednich administratorach, czyli dyrektorach wydziałów sportu, wydziałów oświaty oraz szkół, a także mieszkańców będących użytkownikami infrastruktury rekreacyjnej. Pomaga w koordynowaniu wynajmu poszczególnych obiektów i monitorowaniu efektywności ich użytkowania, a dzięki automatycznemu raportowaniu kadra zarządzająca jednostki publicznej odpowiedzialnej za ich utrzymanie zyskuje dostęp do informacji o stopniu zainteresowania i obłożenia ośrodkami, a także generowanych z tego przy-



Obiekty sportowo-rekreacyjne mogą przynosić zyski, stając się źródłem renowacyjnych inwestycji.

chodach, które mogą stać się dodatkowym źródłem renowacyjnych inwestycji.

> **Informacje o stopniu eksploatacji obiektów i generowanych z tego przychodach mogą stać się dodatkowym źródłem renowacyjnych inwestycji.**

System Obsługi Rezerwacji Obiektów Sportowych posiada również funkcjonalności istotne z punktu widzenia mieszkańców regionu, zainteresowanych korzystaniem z istniejących na jego terenie obiektów rekreacyjnych, hal sportowych, sal gimnastycznych, boisk szkolnych czy Orlików. Z poziomu jednego, dedykowanego portalu stanowiącego HUB dla serwisów poszczególnych szkół i ośrodków, mieszkańcy mają dostęp do aktualnej i kompletnej informacji o dostępnych miejscach sportu i rekreacji. Mają możliwość łatwego i szybkiego wyszukiwania konkretnych placówek, przeglądania kalendarzy ich dostępności i dokonywania rezerwacji w sposób zdalny za pośrednictwem Internetu. Rezerwacje mogą być dokonywane jednorazowo z płatnością online lub w modelu cyklicznym, czyli długoterminowym, ze wskazaniem konkretnych terminów wykorzystania. Dodatkową zaletą przynoszącą korzyści zarówno jednostkom samorządu, jak i mieszkańcom w zakresie komunikacji jest zarządzanie informacją o imprezach sportowych i wydarzeń im towarzyszących, które oznaczone są na kalendarzu będącym integralną częścią portalu.

Z korzyścią dla samorządów i dla mieszkańców

Efektywne zarządzanie infrastrukturą sportową jest istotnym zagadnieniem dla samorządów, które zwracają uwagę na problemy w komunikowaniu o niej do mieszkańców, wyzwania kompetencyjne z zakresu zarządzania, czasochłonność związaną z administrowaniem obiektami, opóźnienia w przepływie informacji na temat ich wynajmu i wynikające z tego utrudnienia w zakresie kontroli stopnia i eksploatacji. Jednak wymienione wyzwania nie muszą stanowić przeszkody nie do pokonania, ponieważ istnieją eliminujące je dedykowane rozwiązania, które umożliwią promocję oferty infrastruktury i zapewnią wsparcie w obszarze administrowania oraz raportowania.

System Obsługi Rezerwacji Obiektów Sportowych to praktyczne narzędzie, które przynosi korzyści samorządom, administratorom i mieszkańcom, usprawniając działanie w zakresie komunikacji i zarządzania infrastrukturą sportową. Wpisuje się w potrzeby i spełnia oczekiwania każdej ze stron, jako element budowanej w obszarze sektora publicznego cyfrowej dostępności, która przekłada się na pozytywny wizerunek jednostek samorządu terytorialnego wśród obywateli, jednocześnie umożliwiając wykorzystanie ekonomicznego potencjału funkcjonujących w regionie obiektów sportowo-rekreacyjnych.

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.

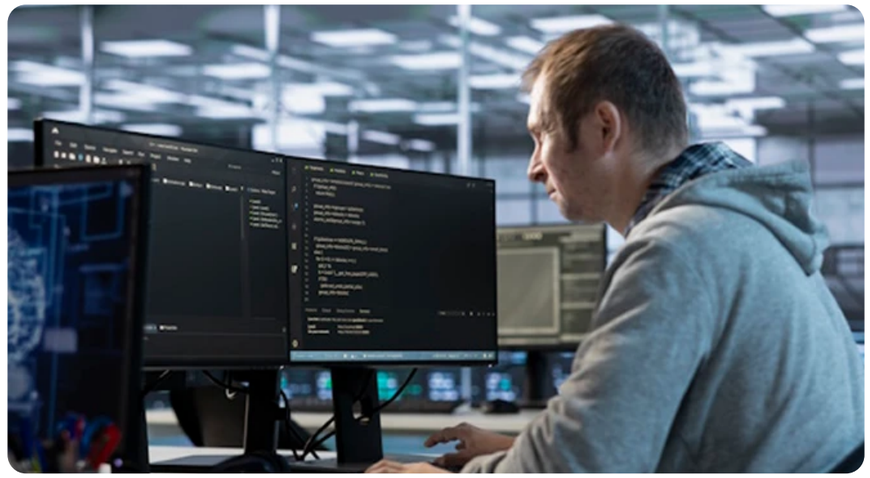
Jak zdalnie i w sposób centralny sprawnie zarządzać wynajmem obiektów sportowo-rekreacyjnych?

Poznaj rozwiązanie i zobacz efekty!

Pobierz bezpłatnie materiał

Jak reagować na incydenty. Standardy właściwej obsługi zdarzeń w środowisku IT

Choć w budowaniu systemów bezpieczeństwa dążymy do minimalizacji ryzyka ataku, to skala zagrożeń z jakimi może spotkać się nasza organizacja sprawia, że dziś właściwym pytaniem nie jest „Czy zostaniemy zaatakowani?", a raczej „Kiedy dojdzie do ataku?". Analogicznie, skuteczny system bezpieczeństwa nie powinien dzisiaj unikać ataków, a potrafić je odpierać. Niestety, nie istnieją w pełni efektywne mechanizmy zabezpieczeń i dlatego równie istotna jest umiejętność reakcji wtedy, kiedy cyberprzestępcy wezmą naszą organizację na celownik. Jak właściwie reagować na incydenty bezpieczeństwa? To nie musi być trudne!



Za właściwy przebieg reakcji na incydenty odpowiada Incident Response Plan (IRP) – to zbiór instrukcji, który określa podstawowe czynności, jakie należy realizować przygotowując się do zdarzenia, podczas niego oraz po jego zakończeniu. Struktura IRP została opracowana i szczegółowo opisana w standardzie ISO/IEC 27035, którego najnowsze wydanie zostało opublikowane w 2023 roku. Norma opisuje przebieg cyklu, który początek ma przed incydentem, zaś kończy się już po jego pełnej obsłudze. Choć standard jest bardzo dobrym wyznacznikiem kierunku budowy IRP, to certyfikacja nie jest niezbędna do tego, aby właściwie zarządzać systemem w dniu ataku. Już dziś warto przygotować się na sytuację kryzysową, a wykonana praca może zaprocentować wtedy, kiedy nasze mechanizmy zabezpieczeń zawiodą.

Czy to był incydent?

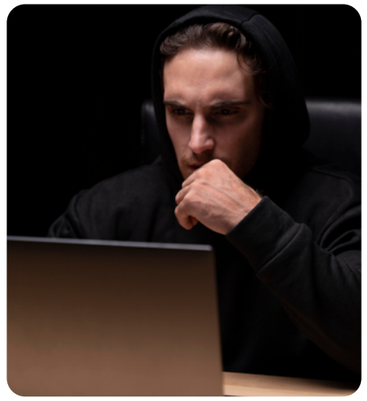
Żeby mówić o obsłudze incydentu musimy wiedzieć, czym on w zasadzie jest. Definicja pojęcia „incydentu bezpieczeństwa" i faktyczne jej zrozumienie to zadanie zaskakująco trudne. Zgodnie z ustawą o Krajowym Systemie Cyberbezpieczeństwa, za incydent należy uznać „zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych". Oznacza to, że incydentem nie jest jedynie skuteczny cyberatak, ale także np. awaria systemu. Jednocześnie, z tego samego dokumentu dowiemy się, że istnieje dodatkowa klasyfikacja incydentów (incydent poważny, incydent krytyczny i incydent w cyberbezpieczeństwie na dużą skalę) – odpowiednie określenie sytuacji, z którą się spotkamy może mieć wpływ na to, w jaki sposób będziemy reagować.

> **Incydentem nie jest tylko skuteczny atak, ale każde potencjalnie niebezpieczne zdarzenie.**

Etap 1 - Przygotowanie

Właściwe przygotowanie do potencjalnego ataku może okazać się bezcenne wtedy, kiedy faktycznie przyjdzie nam zmierzyć się z zagrożeniem. W tym celu konieczne jest precyzyjne zdefiniowanie nie tylko kolejności realizacji zadań, ale także ich celów oraz odpowiedzialności osobowej za ich przebieg. Osoby tworzące zespół reagowania powinny wiedzieć co, kiedy i dlaczego trzeba zrobić. Stworzenie zespołu reagowania oraz definicja obowiązków i odpowiedzialności to właśnie pierwsze z zadań, jakie należy wykonać.

Ważne jest, aby powołany zespół składał się z osób posiadających nie tylko odpowiednie kompetencje, ale i uprawnienia decyzyjne. W sytuacji kryzysowej to właśnie tempo podejmowania kluczowych działań może okazać się kluczowe. W zespole konieczna jest również reprezentacja każdego z obszarów, które w całości tworzą system bezpieczeństwa w warstwie technicznej, administracyjnej, osobowej i fizycznej. Zwyczajowo, grupę nadzoruje także przedstawiciel zarządu niezbędny do podejmowania najważniejszych, zwykle trudnych decyzji. Częstym błędem bywa zbyt rozbudowana grupa odpowiedzialnych za zarządzanie incydentem. Im większy zespół, tym bardziej rozmyta odpowiedzialność i dłuższy proces decyzyjny. Utknięcie w wewnętrznych procesach w sytuacji, w której trwa cyberatak, to jedna z tych sytuacji, której z pewnością chcemy uniknąć.



> **Obsługa incydentu bezpieczeństwa to złożona procedura wymagająca precyzyjnych instrukcji dla wszystkich zaangażowanych.**

Obsługa incydentu bezpieczeństwa to proces wielowątkowy, w którym dążymy do osiągnięcia nie jednego, a szeregu celów, w tym m.in. minimalizacja skutków ataku, zebranie dowodów zdarzenia, spełnienie wymagań prawnych, ograniczenie przestojów, wykrycie i zabezpieczenie luki w systemie. Aby osiągnąć te cele, niezbędne okazują się precyzyjne instrukcje, specyficzne dla wszystkich zaangażowanych w proces. Im bardziej konkretnie określimy kroki procesu, tym lepiej zadziała on w sytuacji, do której został opracowany. W tym zakresie szczególnie istotna jest komplementarność procedur i warstwy technicznej posiadanego systemu bezpieczeństwa. Proceduralne podejście, definicja priorytetów oraz czasów i optymalizacja zadań pozwoli osiągnąć schemat, który najlepiej sprawdzi się w trakcie trwania incydentu. Praca, którą poświęcimy na przygotowanie się do zdarzenia przełoży się na minimalizację konsekwencji i lepszą reakcję na zdarzenie.

Etap 2 – Analityka i detekcja

Aby rozpocząć proces obsługi incydentu, musimy go najpierw zidentyfikować. Niezbędna okazuje się w tym wypadku odpowiednia definicja i umiejętność określenia, w którym momencie faktycznie mamy z nim do czynienia. Źródłem informacji o potencjalnym zagrożeniu może być zarówno system informatyczny, np. narzędzie klasy IDS, SIEM, oprogramowanie antywirusowe bądź inne mechanizmy monitorowania, jak i użytkownik końcowy lub osoba spoza organizacji, która zauważy i zaraportuje anomalię. Wśród najpopularniejszych źródeł informacji o potencjalnych incydentach nie powinniśmy pomijać tych dostępnych publicznie, np. dotyczących wykrytych podatności w użytkowanych systemach.

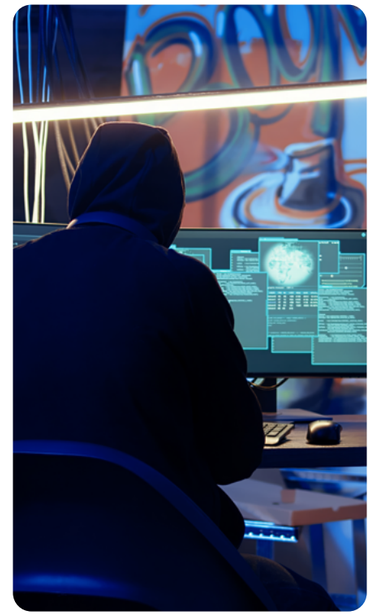
Sygnały dot. zdarzenia określamy jako „sygnały ostrzegawcze" – wskazania, że do ataku może dojść w przyszłości lub „wskaźniki" – informacje, że do ataku doszło lub jesteśmy w jego trakcie. W obu przypadkach konieczne jest podjęcie działań, jednak to wskaźniki stanowią zdecydowanie gorszą wiadomość.

Należy mieć na uwadze, że już pierwsze oznaki mówiące o incydencie powinny być udokumentowane, gdyż mogą one stanowić bezcenną wiedzę w trakcie i po zakończeniu prac. W przypadku ustawy o Krajowym Systemie Cyberbezpieczeństwa to moment powzięcia wiedzy o zdarzeniu wyznacza czas, w jakim powinniśmy poinformować właściwe organy o wykryciu ataku. Identyfikacja incydentu może więc wywoływać inne procesy w naszej organizacji.

Etap 3 – Zarządzanie incydentem

Krytycznym i najbardziej skomplikowanym etapem obsługi incydentu okazuje się proces zarządzania zdarzeniem. To moment, w którym wiemy już, że incydent miał miejsce, powinniśmy również posiadać podstawową wiedzę o potencjalnym wektorze ataku, zakresie skompromitowanych danych czy ewentualnych konsekwencjach. Na tym etapie nasz schemat działania powinien dzielić się na szereg zadań, za które odpowiedzialni są członkowie utworzonego przez nas Incident Response Team.

Na podstawie posiadanych już informacji zespół IT powinien zdefiniować odpowiednią strategię minimalizacji skutków zdarzenia. W tym miejscu dążymy do przerwania ataku (jeśli nadal trwa) poprzez izolację zainfekowanej części środowiska. Istnieją sytuacje, w których struktura zagrożenia zakłada, że ofiara będzie dążyć do przerwania procesu, co wywołuje kolejne złośliwe skrypty – w takich sytuacjach rozwiązaniem jest przeniesienie płaszczyzny ataku na bezpieczne środowiska typu Sandbox.



Równocześnie w procesie obsługi incydentu osoby odpowiedzialne za zainfekowane, uszkodzone bądź skompromitowane systemy powinny dążyć do identyfikacji samego źródła zagrożenia.

> **Wiedza na temat pochodzenia i początkowego punktu detonacji pomaga w eliminacji niebezpieczeństwa.**

Aby skutecznie pozbyć się niebezpieczeństwa, trzeba poznać jego pochodzenie i pierwszy punkt detonacji. To proces niezwykle skomplikowany i często niemożliwy bez odpowiedniego zaplecza technicznego, jednak już samo poszukiwanie może pomóc w wykryciu innych, jeszcze nieaktywnych pułapek.

W trakcie realizacji powyższych działań, niezbędna jest ciągła dokumentacja przebiegu procesu. Wykryte dowody i ślady po zdarzeniu mogą nie tylko pomóc w szybszym uporaniu się z powstałym problemem, ale będą też niezbędne w procesach wynikających z przepisów prawa.

Etap 4 – Eradykacja i odzyskiwanie

Kiedy już uda się wyizolować zagrożenie, należy skupić się na eliminacji jego źródeł i przywracaniu ciągłości działania. Eliminacja zagrożenia powinna dotyczyć każdego elementu infrastruktury, który mógł być dotknięty incydentem. Częstym błędem okazuje się pominięcie w analizie poincydentalnej urządzeń końcowych oraz kopii zapasowych. To te punkty mogą stanowić bezpieczną przystań dla złośliwego oprogramowania, które w przyszłości doprowadzi do kolejnego zdarzenia. Proces eradykacji potencjalnie niebezpiecznych komponentów warto rozpocząć od precyzyjnego określenia wszystkich punktów, do których dostęp mógł mieć potencjalny atakujący. Eliminacja zagrożeń ma zastosowanie wtedy, kiedy incydent jest spowodowany działaniem zewnętrznym i często jest łączona z procesem kompletowania dowodów. Odzyskiwanie środowiska i przywracanie ciągłości działania to proces, który kończy główną fazę obsługi incydentu. Na tym etapie mamy już pełną wiedzę dotyczącą płaszczyzny ataku, jego konsekwencji oraz luk, które do niego doprowadziły. Powinniśmy też być już w trakcie realizacji wszystkich procedur związanych z prawnymi wymogami raportowania. Choć odzyskanie pełni sprawności po incydencie często może trwać bardzo długo, to umiejętne wytypowanie systemów krytycznych dla funkcjonowania organizacji pozwoli odzyskiwać zasoby w odpowiedniej kolejności. Dzięki temu będzie można jak najszybciej wrócić do standardowych zadań, nawet wtedy, kiedy będzie kontynuowane odzyskiwanie.

> **Wiedza, które systemy są krytyczne dla funkcjonowania organizacji, pozwala szybciej powrócić do standardowych zadań.**

Etap V – Lekcja, wnioski i doskonalenie

Odzyskanie dostępności systemów i gwarancja dotycząca całkowitego usunięcia zagrożenia nie kończy procesu obsługi incydentu. Aby skutecznie zamknąć zdarzenie, konieczne jest wyciągnięcie odpowiednich wniosków z sytuacji, w której się znaleźliśmy.

Znając źródło i strukturę zagrożenia, warto niezwłocznie podjąć kroki, które uchronią nas przed takim samym niebezpieczeństwem w przyszłości. Sam przebieg obsługi incydentu również dobrze jest dokładnie przeanalizować i sprawdzić, czy zadziałał prawidłowo i czy nie istnieją obszary, w których można go usprawnić.

Dopiero taka analiza formalnie kończy proces obsługi incydentu. Nie powinna jednak zwalniać z obowiązku doskonalenia, regularnych testów bezpieczeństwa i zewnętrznych analiz, które mogą zidentyfikować luki w zabezpieczeniach. Takie działania to nieodzowny element systemu bezpieczeństwa informacji wdrożonego w organizacji.

> **Faktycznym zakończeniem procesu obsługi incydentu jest analiza podsumowująca procedurę.**

Procedura reagowania i ochrony

Incydent bezpieczeństwa w organizacji zawsze stanowi ogromny problem i wyzwanie, ale właściwe przygotowanie do jego obsługi pomoże w minimalizacji konsekwencji zdarzenia. Należy jednak pamiętać, że aby proces reakcji na incydent zadziałał prawidłowo, musimy wiedzieć, czym on jest i potrafić go zidentyfikować. To właśnie praca, którą wykonamy przed zdarzeniem jest kluczowa i niezależnie, czy i kiedy do incydentu dojdzie, właściwe procedury powinniśmy zbudować już teraz.

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.

Bezpieczna chmura obliczeniowa w urzędzie w dobie cyfryzacji sektora publicznego

Cyfryzacja sektora publicznego to dziś nie tylko rozwój e-usług, ale przede wszystkim odpowiedzialność za dane obywateli, ciągłość działania urzędów oraz spełnienie wymagań prawnych związanych z ich ochroną. Chmura obliczeniowa coraz częściej staje się naturalnym środowiskiem pracy administracji publicznej, jednak jej wykorzystanie wymaga świadomego i przemyślanego podejścia do bezpieczeństwa.

Jednym z fundamentów bezpiecznej chmury jest zarządzanie tożsamością i dostępem. To właśnie na tym poziomie zapada decyzja, kto i na jakich zasadach może korzystać z systemów oraz danych przetwarzanych w urzędzie. W środowisku Microsoft rolę centralnego punktu kontroli dostępu pełni Microsoft Entra ID, który odpowiada za zarządzanie tożsamościami użytkowników oraz zasadami logowania.

Centralne zarządzanie tożsamością pozwala uporządkować dostęp w całym środowisku, od poczty i dokumentów, po systemy, z których pracownicy korzystają na co dzień. Użytkownicy logują się w jednolity sposób, a zasady dostępu są spójne i stosowane w skali całej organizacji. Dzięki temu urząd ma pełną przejrzystość w zakresie tego, kto ma dostęp do konkretnych zasobów i z jakiego powodu.

> **Centralne zarządzanie tożsamością pozwala uporządkować dostęp w całym środowisku.**

Zarządzanie uprawnieniami

Istotnym elementem bezpieczeństwa w administracji publicznej jest również zasada minimalnych uprawnień. Pracownicy powinni mieć dostęp wyłącznie do tych danych i systemów, które są niezbędne do realizacji ich obowiązków służbowych. Ograniczenie nadmiarowych uprawnień zmniejsza ryzyko błędów, nadużyć oraz przypadkowego ujawnienia informacji.

Nowoczesne środowisko chmurowe umożliwia także kontrolę dostępu zależną od kontekstu, a nie wyłącznie od hasła. Decyzje o dostępie mogą uwzględniać m.in. lokalizację użytkownika, rodzaj urządzenia czy poziom ryzyka związanego z logowaniem. Oznacza to, że bezpieczeństwo zaczyna się już na etapie logowania do systemów, zanim użytkownik uzyska dostęp do danych.

Ochrona danych

Jednocześnie bezpieczna chmura to nie tylko pytanie o to, kto ma dostęp do systemów, ale również o to, jakie dane są przetwarzane, gdzie się znajdują i w jaki sposób są chronione. W administracji publicznej są to często dane osobowe, finansowe oraz informacje objęte szczególną ochroną, których właściwe zabezpieczenie ma kluczowe znaczenie dla zaufania obywateli.

W tym obszarze istotną rolę odgrywa Microsoft Purview, który wspiera urzędy w identyfikowaniu i porządkowaniu informacji przetwarzanych w środowisku Microsoft 365. Pozwala on rozpoznawać różne typy danych zarówno wynikające z przepisów prawa, jak i charakterystyczne dla danej jednostki bez konieczności ręcznego oznaczania każdego dokumentu czy pliku.

> **Bezpieczna chmura to nie tylko pytanie o to, kto ma dostęp do systemów, ale również o to, jakie dane są przetwarzane, gdzie się znajdują i w jaki sposób są chronione.**

> **Klasyfikacja informacji stanowi punkt wyjścia do skutecznej ochrony danych.**

Klasyfikacja informacji stanowi punkt wyjścia do skutecznej ochrony danych. Dzięki niej urząd wie, które informacje wymagają podwyższonego poziomu zabezpieczeń i może stosować wobec nich odpowiednie mechanizmy ochrony. Ma to szczególne znaczenie w środowisku, w którym dane są przetwarzane w wielu usługach i przez różnych użytkowników.

Dostęp do danych

Jeśli zarządzanie tożsamością odpowiada za to, kto i na jakich warunkach uzyskuje dostęp do systemów, to kolejnym poziomem bezpieczeństwa jest kontrola tego, co dzieje się z danymi w trakcie codziennej pracy. W tym zakresie Microsoft Purview oferuje mechanizmy zapobiegania utracie danych (Data Loss Prevention), które pozwalają egzekwować zasady postępowania z informacjami wrażliwymi.

Rozwiązania DLP umożliwiają reagowanie na sytuacje, w których dane mogłyby zostać udostępnione w sposób niezgodny z przyjętymi zasadami, na przykład przy próbie przesłania ich poza organizację lub zapisania w nieautoryzowanym miejscu. System może w takich przypadkach ostrzec użytkownika, zablokować działanie lub wymusić dodatkowe potwierdzenie, w zależności od poziomu ryzyka.

Co istotne, te same zasady ochrony danych mogą być stosowane spójnie w różnych usługach, takich jak poczta elektroniczna, dokumenty czy narzędzia współpracy. Dzięki temu ochrona informacji nie zależy wyłącznie od świadomości użytkowników, ale jest wbudowana w sposób działania środowiska.

Podsumowanie

Bezpieczna chmura w sektorze publicznym nie jest jednorazowym wdrożeniem, lecz procesem. Oparcie go o centralne mechanizmy zarządzania tożsamością, dostępem i danymi pozwala budować środowisko, które jest jednocześnie nowoczesne, zgodne z obowiązującymi regulacjami i odporne na współczesne zagrożenia. To właśnie takie podejście stanowi fundament bezpiecznej cyfryzacji urzędu.

Dorota Wysocka

Specjalizuje się w usługach chmurowych Microsoft, pomagając w zrozumieniu i doborze odpowiednich licencji pozwalających efektywnie korzystać z narzędzi Microsoft. Wspiera partnerów i ich klientów w wykorzystywaniu narzędzi Microsoft na co dzień. Wspólnie z partnerami TD SYNNEX dąży do sukcesu, łącząc innowacyjne rozwiązania z praktycznymi potrzebami organizacji.

WCAG 2.2. Nowy standard dostępności cyfrowej portali jednostek sektora publicznego

Wraz z postępującą cyfryzacją wiele usług publicznych zostało przeniesionych do Internetu – od prostych wniosków, poprzez rejestry, na płatnościach kończąc. Jakkolwiek celem rozbudowy zakresu e-usług było ułatwienie obywatelom korzystania z nich, tak w praktyce dla części opcja online mogłaby stanowić utrudnienie. Dotyczy to osób starszych i z niepełnosprawnościami, z myślą o których powstała norma WCAG określająca zasady dostępności cyfrowej i eliminująca ryzyko wykluczenia.

WCAG, czyli Web Content Accessibility Guidelines, to zestaw wytycznych opracowanych przez World Wide Web Consortium (W3C) w ramach inicjatywy WAI (Web Accessibility Initiative). Stanowi podstawę dostępności treści internetowych dla osób z różnymi rodzajami niepełnosprawności, jak wzrokowe, słuchowe, ruchowe oraz poznawcze. Zawiera szereg zaleceń odnośnie projektowania serwisów i aplikacji tak, aby były przejrzyste, czytelne i funkcjonalne. Wskazuje podmioty zobowiązane do stosowania zasad i definiuje konsekwencje związane z ich nieprzestrzeganiem.

13 wytycznych WCAG

Do 2025 roku punktem odniesienia w polskich przepisach była WCAG 2.1, jednak w związku z wejściem w życie European Accessibility Act oraz aktualizacją wytycznych W3C, WCAG 2.2 staje się aktualnym standardem referencyjnym. W stosunku do normy 2.1 wprowadza aż dziewięć nowych kryteriów. Podstawą dla nich są cztery główne zasady – tzw. POUR (Perception, Operability, Understandability, Robustness), w ramach których zdefiniowano 13 wytycznych oraz szczegółowe kryteria sukcesu, których spełnienie podlega ocenie.

01. Tekstowe odpowiedniki dla treści nietekstowych.
02. Zapewnienie dostępności audio i wideo (napisy, audiodeskrypcja).
03. Tworzenie treści w sposób umożliwiający różne formy prezentacji.
04. Ułatwienie widzenia i słyszenia treści (np. kontrast).
05. Dostępność klawiatury (klawisz Tab) eliminująca użycie myszy.
06. Zapewnienie czasu na wykonanie działań (np. formularze, sesje).
07. Eliminowanie efektów (np. migotanie) powodujących napady.
08. Ułatwienie orientacji i poruszania się (menu, nagłówki, fokus).
09. Łatwa interakcja (np. dotyk, kliknięcia) i wprowadzania danych.
10. Czytelne i zrozumiałe informacje (np. język, skróty).
11. Spójne działanie strony, które nie zaskakuje użytkownika.
12. Pomoc w wypełnianiu formularzy (walidacja, alerty błędów).
13. Działanie w różnych przeglądarkach i z technologiami wspomagającymi.

Obowiązek ustawowy

Podmioty publiczne w Polsce, w tym jednostki samorządu terytorialnego i administracji, są zobligowane do zapewnienia dostępności cyfrowej na mocy ustawy z 4 kwietnia 2019 r., co oznacza konieczność spełnienia wymagań WCAG na poziomie AA. Poziom AA, określany jako średni, obejmuje wszystkie wymagania przewidziane dla poziomu A oraz dodatkowe kryteria.

> **WCAG 2.2 to standard opracowany przez W3C, który ma zapewnić prosty, intuicyjny i równy dostęp do informacji oraz e-usług.**

Dotyczą one m.in. odpowiedniego kontrastu, możliwości obsługi serwisu za pomocą klawiatury, dodawania napisów do wideo, stosowania poprawnej semantyki w postaci nagłówków i list, działania strony w orientacji poziomej i pionowej, wielkości elementów dotykowych, obsługi formularzy i prawidłowej nawigacji.

Zgodnie z dyrektywą 2016/2102 obowiązek ten dotyczy serwisów internetowych i aplikacji mobilnych: organów administracji publicznej, jednostek samorządu terytorialnego, instytucji kultury, szkół i uczelni publicznych, sądów i innych organizacji publicznych. Trzeba tu zaznaczyć, że serwisy tworzone po 2019 roku powinny być projektowane już według zasad WCAG, a starsze wymagają dostosowania do standardów wskazanych normą.

Poziom dostępności

Pełna zgodność serwisów sektora publicznego z normą WCAG wciąż jest rzadkością – dominują wdrożenia częściowe kryteriów dostępności cyfrowej. Braki najczęściej odnotowywane są w obszarze struktury i treści serwisu, gdzie dotyczą tekstów alternatywnych i nagłówków. Problemem okazuje się też niedostateczny kontrast między tłem a tekstem czy elementami grafiki. Zdarzają się również utrudnienia przy obsłudze formularzy czy odnajdywaniu dokumentów oraz multimediów. Jednak z roku na rok wskaźnik poprawności WCAG rośnie, a podobne nieprawidłowości są eliminowane.

Dedykowane narzędzia

Procedura zarządzania dostępnością jest procesem wymagającym – pod względem wiedzy, kompetencji i narzędzi. Te ostatnie mogą okazać się pomocne. Przykładowo, Platforma Multiportalowa PUBLIC web360 posiada funkcjonalności, które pomagają redaktorom w tworzeniu dostępnych cyfrowo portali internetowych. Wbudowane walidatory umożliwiają sprawdzenie poprawności tworzonych treści i szablonów w zakresie: kolejności nagłówków, opisów alternatywnych grafik i linków, kontrastu tekstu, poprawności tabel i innych aspektów. Pozwalają na dodawanie audiodeskrypcji do plików wideo i blokowanie możliwości dodania grafiki z brakującym atrybutem alt. W połączeniu z AI dostępne w panelu walidatory automatycznie generują określone treści, a także wskazują i naprawiają błędy, co prowadzi do oszczędności czasu. System nie pozwoli dodać wpisu do portalu z wykrytym błędem dostępności, a narzędzia AI pomogą go automatycznie poprawić.

> **Zewnętrzny audyt potwierdził dostępność cyfrową platformy PUBLIC web360 także po stronie panelu administracyjnego.**

Zaletą platformy jest „Moduł deklaracji dostępności", umożliwiający intuicyjne tworzenie zgodnej z obowiązującymi warunkami technicznymi deklaracji dostępności oraz globalny podgląd statusów dostępności wszystkich portali z opcją raportu zbiorczego. Jest to pomocne dlatego, że każdy podmiot publiczny ma obowiązek publikowania aktualnej deklaracji dostępności swoich serwisów w zakresie wymogów WCAG. Tymczasem zdarzają się sytuacje, że brakuje tej wymaganej ustawowo dokumentacji.

Konsekwencje prawne

Wraz z obowiązkiem monitorowania i raportowania stanu dostępności cyfrowej wprowadzono prawne konsekwencje w przypadku niespełnienia wymogów. Podmiot publiczny może ponieść karę finansową, jeśli jego serwis nie spełnia wymagań dostępności cyfrowej opartych o standard WCAG (aktualnie w wersji 2.2 jako standard referencyjny), nie opublikował deklaracji dostępności lub nie zareagował na skargi. W ostatnim przypadku użytkownik ma prawo zgłosić naruszenia, a podmiot jest zobligowany wziąć je pod uwagę.

Nadzór nad przestrzeganiem zasad pełni w Polsce kilka podmiotów. W przypadku sektora publicznego:

- Prezes Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych – przyjmuje skargi o naruszeniach dostępności cyfrowej i prowadzi postępowania kontrolne,
- Ministerstwo Cyfryzacji i organy nadrzędne w stosunku do jednostek samorządu terytorialnego, urzędów, szkół i szpitali.

Jakość cyfrowych usług

Obowiązująca już od kilku lat norma WCAG to nie tylko zestaw wytycznych technicznych, według których należy projektować serwisy i aplikacje. Wprowadzona w 2025 roku wersja 2.2 jasno pokazuje, że celem jest zapewnienie odpowiedniego standardu jakości usług cyfrowych. Wymaga on tworzenia stron i aplikacji o czytelnych treściach, prostej nawigacji, intuicyjnych interfejsach dostosowanych do urządzeń mobilnych, aby każdy użytkownik mógł szybko odnaleźć informacje i łatwo załatwić sprawę w sposób zdalny.

Damian Stanisławczyk

Product owner i projektant rozwiązań wpisujących się w specyfikę rynku oraz oczekiwania klientów. Dzięki stałej analizie trendów sektora publicznego i wiedzy na temat potrzeb instytucji kreuje funkcjonalności zapewniające interesariuszom realne korzyści.

Bezpieczeństwo przetwarzania danych osobowych w kontekście rozwiązań hostingowych

W dobie postępującej cyfryzacji i w obliczu rosnącej liczby cyberzagrożeń dane stają się kluczowym zasobem wymagającym zwiększonej ochrony. Dla instytucji publicznych jest to szczególne wyzwanie ze względu na charakter przetwarzanych informacji i specyfikę organizacyjną samego podmiotu. Wszelkie naruszenia mogą zaszkodzić tak obywatelom, jak i instytucji, niosąc ryzyko utraty reputacji, odpowiedzialności prawnej i kar finansowych.

Bezpieczeństwo informacji i ochrona danych to jedno z kluczowych wyzwań transformacji cyfrowej sektora publicznego. Instytucje, zwłaszcza jednostki samorządu terytorialnego przetwarzają bardzo szeroki zakres informacji od danych osobowych obywateli, poprzez zdrowotne i finansowe, aż po te o infrastrukturze krytycznej. Pozostają one rozproszone w wielu systemach – jak ERP i dziedzinowe, EZD, ePUAP czy inne aplikacje, które zazwyczaj pochodzą od różnych dostawców. Powstaje w ten sposób mozaika rozwiązań, która utrudnia integrację systemów, nadzór nad przepływami danych oraz jednolite zarządzanie bezpieczeństwem. Rodzi to konieczność stosowania zróżnicowanych poziomów ochrony.

Ochrona danych zgodnie z prawem

Ze względu na charakter przetwarzanych informacji oraz rosnącą skalę cyberzagrożeń podmioty sektora publicznego podlegają wielu regulacjom prawnym. Zarówno przepisom RODO, które określają zasady ochrony danych osobowych, jak i ustawie o KSC, która nakłada obowiązki w zakresie zarządzania cyberbezpieczeństwem, reagowania na incydenty i zapewnienia ciągłości działania systemów. Do tego dochodzą jeszcze inne regulacje, m.in. ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne, przepisy dotyczące Krajowych Ram Interoperacyjności, a także odnoszące się do dostępu do informacji publicznej, archiwizacji dokumentacji oraz zamówień publicznych.

Wobec tak rozbudowanych aktów prawnych podmioty sektora publicznego muszą zadbać o kompleksowe i zgodne z prawem utrzymanie systemów przetwarzania danych, obejmujące zarządzanie ryzykiem, wdrożenie adekwatnych środków technicznych i organizacyjnych, zapewnienie ciągłości działania, skuteczne procedury reagowania na incydenty, a także nadzór nad dostawcami usług hostingowych oraz prowadzenie dokumentacji potwierdzającej zgodność z obowiązującymi przepisami.

> **Dane w sektorze publicznym są dziś zasobem krytycznym, a ich naruszenie oznacza nie tylko ryzyko prawne i finansowe, lecz także realne zagrożenie dla zaufania obywateli do instytucji.**

W ramach własnego data center

Pogodzenie wymagań prawnych w celu zapewnienia bezpieczeństwa systemów i danych wymaga połączenia kompetencji organizacyjnych, prawnych i technicznych. W przypadku utrzymywania serwerowni we własnym zakresie ciężar odpowiedzialności spoczywa na wewnętrznych działach IT lub na pojedynczych informatykach odpowiedzialnych za działanie infrastruktury. Do ich zadań należy nie tylko zapewnienie wydajności i stabilności środowiska, w którym działają systemy ERP, kadrowe, księgowe, geodezyjne i inne aplikacje dziedzinowe, lecz także administrowanie serwerami, siecią, kopiami zapasowymi, aktualizacjami, kontrolą dostępu, monitoringiem bezpieczeństwa oraz reagowaniem na incydenty i awarie. Mimo że własna serwerownia daje podmiotom publicznym większą bezpośrednią kontrolę nad infrastrukturą, to równocześnie wymaga stałej dostępności zasobów kadrowych i finansowych.

Dlatego niektóre podmioty decydują się powierzyć całość lub część zadań związanych z utrzymaniem serwerowni firmie zewnętrznej. W takim przypadku dostawca przejmuje określony umową zakres obowiązków, co jednak nie zwalnia jednostki z odpowiedzialności za zgodność z przepisami. Korzystanie z usług zewnętrznych wymaga wyboru kompetentnego dostawcy, a także stałego nadzoru nad realizacją usługi i jasnego podziału odpowiedzialności.

Jednak w obu przypadkach równie istotna jest weryfikacja standardów bezpieczeństwa, potwierdzająca spełnianie wymogów w zakresie ochrony informacji, ciągłości działania, odporności infrastruktury oraz reagowania na incydenty.

W modelu usług hostingowych

Alternatywą dla własnych serwerowni są usługi hostingowe, z których podmioty sektora publicznego korzystają już od lat, przede wszystkim na potrzeby utrzymania portali internetowych, Biuletynów Informacji Publicznej czy wybranych systemów dziedzinowych. Coraz częściej model ten obejmuje również rozwiązania bardziej złożone, związane z elektronicznym zarządzaniem dokumentacją. Przykładem jest rozwijany przez NASK i Ministerstwo Cyfryzacji system EZD RP czy obiegi dokumentów innych dostawców oferujących wraz z rozwiązaniem jego utrzymanie w prywatnej chmurze. Usługi hostingowe pozwalają również spełnić zasadę 3-2-1 związaną z zabezpieczeniem kopii zapasowych, które powinny być przechowywane w trzech wersjach, na dwóch różnych nośnikach, w tym również poza lokalizacją, odseparowane offline.

W praktyce usługi hostingowe pozwalają przenieść na dostawcę znaczną część obowiązków związanych z utrzymaniem infrastruktury, takich jak zapewnienie dostępności środowiska, aktualizacji, kopii zapasowych, wysokiej dostępności czy monitorowania bezpieczeństwa. Dla jednostek sektora publicznego oznacza to możliwość ograniczenia kosztów utrzymania własnej serwerowni i zmniejszenia obciążenia własnych zasobów kadrowych, przy jednoczesnym zachowaniu stałego nadzoru nad zgodnością usługi z przepisami prawa, poziomem bezpieczeństwa oraz warunkami umownymi. W większości przypadków dostawcy hostingu i chmury dysponują niezbędnymi mechanizmami zabezpieczającymi, jak szyfrowanie danych czy systemy ochrony i wykrywania zagrożeń SIEM, procedury Disaster Recovery. Zapewniają również stały monitoring, testy odporności i penetracyjne, regularną weryfikację kopii zapasowych oraz zdolność szybkiego reagowania na incydenty.

Suwerenność technologiczna

W kontekście usług hostingowych szczególnego znaczenia nabiera korzystanie z oferty krajowych dostawców. Nie chodzi wyłącznie o fizyczną lokalizację serwerów, lecz o możliwość kontrolowania miejsca przetwarzania danych, warunków dostępu do nich, zasad świadczenia usługi i cyfrowej suwerenności.

> **Wybór krajowego dostawcy hostingu to nie tylko kwestia lokalizacji serwerów, ale także większej kontroli nad danymi, przejrzystości odpowiedzialności i szybszej reakcji na incydenty.**

Współpraca z krajowymi dostawcami może wzmacniać kontrolę nad tym, gdzie i w jaki sposób przetwarzane są dane obywateli. Nie bez znaczenia jest również łatwiejszy kontakt operacyjny, wsparcie techniczne w języku polskim, większa przejrzystość odpowiedzialności oraz możliwość szybszego reagowania na incydenty i potrzeby instytucji.

Trend outsourcingu

Outsourcing utrzymania systemów

> **Hosting ogranicza koszty utrzymania serwerowni i obciążenie zasobów kadrowych.**

w sektorze publicznym nie jest już nowym trendem, lecz coraz częściej świadomym wyborem organizacyjnym, wynikającym z rosnących wymagań prawnych, technologicznych i kadrowych. Hosting odciąża jednostki publiczne od części obowiązków infrastrukturalnych tak związanych z zarządzaniem, jak i utrzymaniem czy modernizacją sprzętu i oprogramowania serwerowego. Może też zwiększać bezpieczeństwo, dostępność i odporność usług, ponieważ dostawcy usług chmurowych często dysponują rozwiązaniami, które mogą zabezpieczyć środowisko klienta, gwarantując poufność i integralność danych. Dodatkowo, współpraca z krajowymi, certyfikowanymi dostawcami, wspiera nie tylko cyberbezpieczeństwo, ale także suwerenność technologiczną.

Marcin Bryk

Ekspert ds. bezpieczeństwa systemów i audytor wiodący normy 27001. Specjalizuje się w zarządzaniu systemami operacyjnymi i migracją danych do rozwiązań chmurowych. Posiada szeroką wiedzę na temat narzędzi zwiększających bezpieczeństwo sieci i zapewniających ochronę danych, pomagając dbać o bezpieczeństwo infrastruktury IT.

ZFŚS w erze cyfrowej. Jak ograniczyć biurokrację i zwiększyć kontrolę nad funduszem socjalnym?

W wielu jednostkach samorządu terytorialnego ZFŚS wciąż obsługiwany jest w modelu tradycyjnym. Papierowe wnioski krążą między biurkami, dane żyją w arkuszach Excel, decyzje zapisują się w mailach, a działy kadr i komisje socjalne próbują utrzymać nad tym pełną kontrolę. Tymczasem rośnie presja prawna, organizacyjna i pracownicza. W związku z tym fundusz socjalny coraz częściej potrzebuje cyfrowego zaplecza, które porządkuje proces, wzmacnia transparentność i pozwala jasno pokazać, że każda decyzja została podjęta według określonej procedury.

Choć zasady funkcjonowania ZFŚS są określone przepisami i regulaminami wewnętrznymi, w praktyce proces ten rzadko pozostaje w pełni uporządkowany. Dla większości działów HR i komisji socjalnych w JST obsługa funduszu to wypadkowa wielu równoległych działań, realizowanych przez różne osoby, przy użyciu różnych narzędzi.

Obsługa ZFŚS w praktyce

Jednym z największych wyzwań obsługi ZFŚS jest rozproszenie danych. Wnioski, oświadczenia i decyzje funkcjonują jednocześnie w dokumentacji papierowej, arkuszach kalkulacyjnych i korespondencji mailowej. Odtworzenie pełnej historii sprawy wymaga sięgania do wielu źródeł, a ryzyko zagubienia dokumentu lub pominięcia aktualizacji jest stale obecne.

Równie problematyczny pozostaje brak transparentności procesów decyzyjnych. Przy manualnej obsłudze, bez automatycznych wyliczeń i jasno zdefiniowanych reguł, rośnie ryzyko błędów i trudno o śledzenie statusu sprawy w czasie rzeczywistym. Rodzi to obciążenie operacyjne. Każdy wniosek wymaga ręcznej analizy danych, ich przeliczenia zgodnie z kryterium socjalnym i fizycznego przekazania między uczestnikami procesu. W urzędzie zatrudniającym kilkuset pracowników oznacza to kilkadziesiąt lub kilkaset wniosków rocznie, obsługiwanych najczęściej przez ten sam, nieduży zespół kadrowy.

Wiele zmienia automatyzacja

Cyfrowe zarządzanie ZFŚS nie jest tylko kwestią wygody. To zmiana strukturalna, która wpływa na jakość, spójność i bezpieczeństwo całego procesu. Kluczowym elementem jest standaryzacja procedury oraz centralizacja danych i dokumentacji. Gdy wszystkie wnioski, oświadczenia, decyzje i historia świadczeń gromadzone są w jednym miejscu, znika problem rozproszonej informacji. Pracownicy mogą sprawdzać dostępne świadczenia i status spraw online, działy HR mają bieżący dostęp do raportów, a komisja socjalna do aktualnych zestawień.

Istotną zmianę przynosi automatyczne naliczanie świadczeń według kryterium socjalnego. Wnioski są automatycznie przypisywane do odpowiednich progów, uwzględniając sytuację życiową, rodzinną i materialną pracownika. Ten sam dochód na członka rodziny zawsze skutkuje tą samą wysokością świadczenia, bez konieczności manualnego naliczania i ryzyka związanych z tym nieprawidłowości.

Największą wartością cyfryzacji procesów socjalnych nie jest automatyzacja sama w sobie, ale odzyskanie pełnej przejrzystości i kontroli nad tym, jak faktycznie przebiega procedura. Automatyzacja nie zmienia bowiem zasad ZFŚS, lecz sposób, w jaki organizacja jest w stanie je konsekwentnie stosować i egzekwować. To właśnie ten element w praktyce odróżnia cyfryzację, która tylko wspiera proces, od tej, która realnie go porządkuje i standaryzuje.

Większa transparentność procesu

Cyfrowy obieg wniosków i akceptacji oznacza, że wniosek złożony przez pracownika online automatycznie trafia do właściwych osób zgodnie z ustalonym procesem. Eliminuje to konieczność fizycznego obiegu dokumentów, skraca czas obsługi i ogranicza ryzyko zaginięcia czy przeoczenia wniosku. Na każdym etapie dostępny jest aktualny status sprawy.

> **Największą wartość nowoczesnego podejścia do zarządzania ZFŚS stanowi nie tyle automatyzacja sama w sobie, co odzyskanie kontroli i przejrzystości.**

Ważnym aspektem jest też pełna ścieżka audytu. Każda decyzja jest rejestrowana, więc wiadomo kto ją podjął, kiedy i na jakiej podstawie. W przypadku kontroli lub audytu zewnętrznego organizacja ma do dyspozycji kompletną historię działań, możliwą do odtworzenia bez żmudnego przeszukiwania archiwów.

W kontekście cyfryzacji nie można pominąć kwestii bezpieczeństwa danych. Procesy ZFŚS obejmują przetwarzanie wrażliwych informacji o sytuacji rodzinnej i materialnej pracowników. Rozproszone pliki i lokalne arkusze Excel zwiększają ryzyko nieuprawnionego dostępu. Z kolei rozwiązania cyfrowe pozwalają uporządkować zasady dostępu do informacji i wspierają organizację w realizacji obowiązków wynikających z RODO.

Zgodnie z literą prawa

W obszarze ZFŚS zgodność z przepisami nie może opierać się wyłącznie na ręcznej weryfikacji i znajomości regulacji przez poszczególnych pracowników. Powinna być wspierana przez rozwiązania systemowe, które pomagają stosować obowiązujące zasady w sposób jednolity i powtarzalny.

ZFŚS funkcjonuje w oparciu o ustawę z dnia 4 marca 1994 r., która nakłada na pracodawców obowiązek konsekwentnego stosowania kryterium socjalnego przy przyznawaniu świadczeń. Ostatnia nowelizacja przepisów, z 26 stycznia 2026 roku, jeszcze mocniej akcentuje potrzebę uporządkowania procesów wewnętrznych oraz doprecyzowania zasad współpracy z przedstawicielami pracowników — szczególnie w organizacjach, w których nie działają związki zawodowe.

Jakkolwiek cyfrowe narzędzie nie zastępuje regulaminu ZFŚS, tak egzekwuje jego właściwe stosowanie. Automatyzuje kluczowe elementy procesu, wymusza stosowanie przyjętych reguł i zapewnia pełną ścieżkę audytu dla podejmowanych decyzji. Dzięki temu organizacja może skuteczniej ograniczać ryzyko niezgodności z przepisami i budować zaufanie do sposobu dystrybucji środków funduszu.

Wymierne korzyści cyfryzacji

Wdrożenie cyfrowego systemu obsługi ZFŚS przekłada się na wymierne efekty organizacyjne. Z perspektywy działów HR najważniejszy jest czas obsługi, który dzięki automatyzacji naliczeń i samoobsłudze pracowników można znacząco skrócić. Równocześnie zmniejsza się zaangażowanie kadry w obsługę funduszu, co oznacza realne odciążenie zespołów, które zyskują przestrzeń na działania wymagające oceny i decyzji.

> **Cyfryzacja nie zmienia zasad funduszu, lecz sposób, w jaki organizacja jest w stanie je konsekwentnie stosować, dokumentować i egzekwować.**

Widoczne są również oszczędności kosztowe, głównie ze względu na eliminację papierowego obiegu dokumentów, usprawnienie obsługi pożyczek i rozliczeń oraz ograniczenie ryzyka błędów, które w przypadku kontroli mogą generować dodatkowe koszty i obciążenia. Do tego dochodzi wygoda. Możliwość składania wniosków online, bieżący podgląd statusu spraw i jasne zasady przyznawania świadczeń budują pozytywne doświadczenia pracowników samorządowych w kontakcie z pracodawcą.

Elastyczny sposób na zmianę

Tak przedstawiony model automatyzacji można realizować na platformie low-code nAxiom, która pozwala elastycznie odwzorować regulamin ZFŚS w działającym procesie – od obiegu wniosków, przez reguły naliczania świadczeń, po ścieżki akceptacji i raportowanie. Istotna jest również elastyczność systemu wobec zmian prawa. Dzięki podejściu low-code zmiany w zasadach, progach dochodowych czy typach dostępnych świadczeń mogą być wprowadzane szybciej, bez konieczności budowania rozwiązania od podstaw, mocnego angażowania działu IT lub prowadzenia rozbudowanych prac programistycznych.

ZFŚS przestał być wyłącznie formalnością administracyjną. To proces, który musi jednocześnie spełniać wymagania prawne, odpowiadać na oczekiwania pracowników i być gotowy na kontrolę w każdej chwili. W jednostkach samorządu terytorialnego, gdzie skala zatrudnienia i presja na transparentność są szczególnie wysokie, tradycyjne narzędzia przestają być wystarczające. Zyskują te, które dają możliwość automatyzacji z zapewnieniem elastyczności.

Mateusz Szwajkosz

Specjalista w dziedzinie technologii low-code i projektowania oraz budowy opartych na niej rozwiązań. Dysponując wiedzą na temat możliwości cyfryzacji, podpowiada, jak wykorzystywać jej potencjał z korzyścią dla organizacji.

Cyberbezpieczeństwo w centrum uwagi. Relacja z CyberSummIT Podkarpacie 2026

23 kwietnia 2026 roku Jasionka stała się miejscem rozmowy o jednym z najważniejszych wyzwań współczesnych organizacji. Podczas konferencji CyberSummIT Podkarpacie 2026 przedstawiciele sektora publicznego i prywatnego spotkali się, aby wspólnie przyjrzeć się zagadnieniom cyberbezpieczeństwa, ochrony danych oraz zapewnienia ciągłości działania systemów IT w coraz bardziej wymagającym środowisku cyfrowym.

Wydarzenie miało charakter nie tylko ekspercki, lecz także networkingowy, stając się przestrzenią wymiany doświadczeń między decydentami, praktykami i specjalistami, którzy dzielili się wiedzą podczas paneli, prelekcji oraz dyskusji. Konferencję otworzył Tomasz Ostrowski, Prezes Spółki OPTeam, organizatora wydarzenia. Wśród osób inaugurujących znaleźli się również Marcin Deręgowski, Zastępca Prezydenta Miasta Rzeszowa, oraz Karol Ożóg, Wicemarszałek Województwa Podkarpackiego.

Rozmowy, które wychodziły poza scenę

W wydarzeniu CyberSummIT Podkarpacie 2026 uczestniczyły osoby odpowiedzialne za bezpieczeństwo informacji, zarządzanie IT i rozwój infrastruktury cyfrowej w organizacjach publicznych oraz prywatnych. Obecni byli również ci, którzy na co dzień obserwują, jak szybko rośnie skala zagrożeń i jak duże znaczenie ma dziś skuteczna ochrona danych oraz systemów. Z rozmów prowadzonych podczas wydarzenia wybrzmiewał jeden wspólny wniosek. Mianowicie, cyberatak przestał być wyłącznie problemem technicznym, ponieważ jego skutki coraz częściej obejmują całą organizację, wpływając na jej stabilność i ciągłość działania. Dlatego kwestie bezpieczeństwa to już nie tylko kwestie informatyczne, ale również zarządcze, jako element strategii, zarządzania ryzykiem i budowania odporności organizacyjnej. Właśnie to przesunięcie perspektywy było mocno widoczne zarówno podczas oficjalnych wystąpień, jak i w mniej formalnych rozmowach uczestników.

> **Dziś o cyberbezpieczeństwie nie mówi się już wyłącznie w kontekście technologii, lecz konkretnych decyzji o budowie odporności, od których zależy stabilność całych organizacji.**

Dwie sesje, wiele perspektyw

Program konferencji podzielono na dwie sesje merytoryczne, w których eksperci podejmowali tematy związane z bezpieczeństwem cyfrowym, odpornością organizacji i reagowaniem na incydenty. Każda z nich prezentowała inny punkt widzenia, ale razem tworzyły spójny obraz wyzwań, z jakimi mierzą się dziś instytucje i firmy.

Pierwsza część wydarzenia koncentrowała się wokół zagadnienia cybersuwerenności. Eksperci rozmawiali o nim podczas panelu *„Znaczenie lokalnych technologii w procesie budowania cyfrowej niepodległości”*, a temat ten wybrzmiał również w wystąpieniach poświęconych *„Optymalizacji procesów bezpieczeństwa: jak automatyzacja i sztuczna inteligencja wspierają rozwój nowoczesnych zespołów SOC”* oraz *„Jeden strumień danych, dwa światy: network traffic observability jako fundament NOC i SOC”*. W drugiej części uwaga uczestników skupiła się przede wszystkim na nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa. Odniesiono się do niej zarówno w panelu *„Od incydentu do odbudowy: reagowanie, ciągłość i minimalizacja skutków w cyberbezpieczeństwie”*, jak i podczas prelekcji *„Cyberbezpieczeństwo pod presją: jak uKSC zmienia zasady gry i wymusza wdrożenie procedur oraz inwestycje technologiczne”*.

Dlaczego takie spotkania są dziś potrzebne

W realiach, w których każda organizacja może stać się celem ataku, znaczenie podobnych spotkań stale rośnie. Wymiana wiedzy, doświadczeń i dobrych praktyk nie jest już jedynie wartością dodaną, lecz staje się jednym z elementów budowania odporności na cyberzagrożenia. Konferencja CyberSummIT Podkarpacie 2026 pokazała, że rozmowa o ochronie infrastruktury IT i danych nie dotyczy wyłącznie specjalistów, ale coraz częściej angażuje także osoby odpowiedzialne za strategiczne decyzje. To właśnie połączenie perspektywy technologicznej, prawnej i organizacyjnej sprawiło, że wydarzenie stało się ważnym forum dla wszystkich, którzy chcą świadomie odpowiadać na wyzwania cyfrowego świata.

Strategiczny wymiar cyberbezpieczeństwa

CyberSummIT Podkarpacie 2026 pozostawił po sobie coś więcej niż zestaw eksperckich tez i branżowych rekomendacji. Pokazał, że w świecie nieustannej cyfrowej zmiany bezpieczeństwo staje się wspólną odpowiedzialnością nie tylko działów IT, lecz całych organizacji, w tym ich liderów. Podobne spotkania mają dziś znaczenie, bo aktualizują wiedzę i wzmacniają świadomość, przypominając, że odporność organizacji buduje się nie w momencie kryzysu, ale wcześniej poprzez wiedzę, gotowość i współpracę.

Czy właśnie takie spotkania i wspólna wymiana wiedzy mogą dziś przesądzać o realnej odporności organizacji na cyberzagrożenia?

W ostatnich latach wyraźnie widać, że cyberataki stają się coraz bardziej dynamiczne i zaawansowane, a ich sprawcy sięgają po coraz skuteczniejsze metody działania. W takiej rzeczywistości osoby odpowiedzialne za bezpieczeństwo IT muszą nie tylko trafnie wyznaczać priorytety, ale również świadomie i konsekwentnie zarządzać ryzykiem. W OPTeam dobrze znamy skalę tych wyzwań. Dzięki wieloletniej współpracy z instytucjami publicznymi i firmami wiemy, jak projektować rozwiązania odpowiadające na konkretne potrzeby i realne zagrożenia. Z tej właśnie potrzeby narodził się CyberSummIT — konferencja, która integruje środowisko ekspertów odpowiedzialnych za cyberbezpieczeństwo. Jesteśmy przekonani, że otwarta debata i wymiana doświadczeń to dziś jeden z warunków skutecznej ochrony w cyfrowej rzeczywistości.

Aleksander Maziarz,
Dyrektor Obszaru Cyberbezpieczeństwa i Infrastruktury IT w OPTeam SA

Jakie najważniejsze wyzwania w cyberbezpieczeństwie wybrzmiały podczas konferencji?

Konferencja CyberSummIT Podkarpacie 2026 wyraźnie pokazała, że organizacje coraz dojrzalej podchodzą do tematu cyberbezpieczeństwa. Dziś nie chodzi już wyłącznie o zakup kolejnych narzędzi, ale o wyzwanie związane z budowaniem realnej odporności organizacyjnej, opartej nie tylko na technologii, ale także na uporządkowanych procesach, świadomych decyzjach i spójnym środowisku IT. Mocnym echem na konferencji odbił się również temat suwerenności technolo-

Materiały konferencyjne

gicznej, który w dobie napięć geopolitycznych i unijnych regulacji stanowi gigantyczne wyzwanie dla sektora IT. Zagadnienie to coraz częściej wychodzi poza warstwę deklaracji i zaczyna realnie wpływać na sposób projektowania środowisk IT oraz wybór partnerów technologicznych. Nie mówimy już tylko o ochronie przed zagrożeniami, ale o strategicznej niezależności i dojrzałości biznesowej. Najbliższe lata zmuszą nas do porzucenia doraźnych działań na rzecz długofalowej strategii, w której cyfrowe bezpieczeństwo staje się filarem stabilności i przewagi rynkowej.

Grzegorz Filarowski,
Chief Executive Officer, LOG Plus

Czym ta konferencja różni się od innych wydarzeń o cyberbezpieczeństwie?

Konferencja CyberSummit Podkarpacie 2026 wyróżniała się na tle innych wydarzeń o cyberbezpieczeństwie przede wszystkim przesunięciem akcentów – z prezentacji technologii na realne, strategiczne wnioski. Duży nacisk położono na temat cybersuwerenności, która dziś nabiera coraz większego znaczenia w kontekście niezależności technologicznej i bezpieczeństwa państwa oraz organizacji. Konferencja oferowała również rzadko spotykaną jakość merytorycznej debaty – zamiast ogólnych deklaracji pojawiła się konkretna, pogłębiona dyskusja o rozwiązaniach bezpieczeństwa i ich praktycznym zastosowaniu. Istotnym elementem było także podkreślenie, że lokalne kompetencje i technologie stoją na bardzo wysokim poziomie i mogą skutecznie konkurować na rynku. Najważniejsze jednak było to, że prawdziwymi bohaterami wydarzenia byli uczestnicy – ich doświadczenia, pytania i perspektywa, a nie sami prowadzący. Dzięki temu konferencja miała autentycznie dialogowy charakter i realną wartość dla wszystkich zaangażowanych.

Wojciech Pilarski,
Technical Solutions Engineer, Arrow ECS

Jakie znaczenie ma współpraca między sektorem publicznym i prywatnym?

Współpraca sektora publicznego i prywatnego to fundament nowoczesnego ekosystemu cyberbezpieczeństwa, co zostało wielokrotnie podkreślone podczas kwietniowej konferencji CyberSummIT. Bardzo istotne jest partnerskie połączenie misji i zakresu działania administracji z wiedzą technologiczną biznesu. Bliskie współdziałanie obu sektorów, szczególnie na poziomie regionalnym, ma istotny wpływ na bezpieczeństwo codziennych usług i pozwala na skuteczne budowanie cyberodporności. Kluczowym zagadnieniem w kontekście wyzwań związanych z zapewnieniem bezpieczeństwa danych oraz przestrzegania regulacji prawnych w tym zakresie jest identyfikacja ryzyk i odpowiednie postępowanie z nimi. Rzetelna analiza ryzyka pozwala obu partnerom właściwie optymalizować procedury oraz wdrażać adekwatne środki ochrony przeciw cyberzagrożeniom – zarówno techniczne, jak i organizacyjne.

Marcin Stankiewicz,
Specjalista ds. Cyberbezpieczeństwa, SecureVisio

Jakie główne przesłanie uczestnicy wynieśli ze sobą po konferencji?

Główne przesłanie po CyberSummIT? Kluczem do nowoczesnego cyberbezpieczeństwa jest synergia i technologiczna suwerenność. Konferencja jasno pokazała, że działy NOC i SOC nie mogą już działać w silosach – fundamentem skutecznej ochrony jest jeden, precyzyjny strumień danych, co jako Sycope udowodniliśmy na scenie. W dobie AI i rygorystycznych regulacji, takich jak uKSC, wygrywają rozwiązania elastyczne, które pozwalają zachować pełną kontrolę nad własną infrastrukturą sieciową.

Ogromna w tym zasługa lokalnych technologii, które realnie budują naszą cyfrową niepodległość. Cieszę się, że te kluczowe dla rynku wnioski płyną właśnie stąd. Na zaproszenie OPTeam po raz kolejny z wielką przyjemnością odwiedziłem Rzeszów – a powrót w rodzinne strony i dyskusje w tak profesjonalnym gronie to dla mnie zawsze podwójna satysfakcja.

Piotr Kawa,
VP of Sales, Sycope

Magdalena Tobiasz

Ekspertka w zakresie promocji i analityki. Zajmuje się pozyskiwaniem i weryfikacją danych z narzędzi statystycznych na potrzeby strategii wizerunkowych i efektywnościowych. Monitoruje trendy i wydarzenia w celu interpretacji zmian oraz zjawisk rynkowych.

Aleksandra Stachowicz

Ekspertka w dziedzinie komunikacji i promocji, specjalizująca się w strategiach marketingowych i public relations. Wspiera kreowanie wizerunku poprzez budowanie i utrzymywanie relacji, realizuje kampanie eventowe wizerunkowe, informacyjne i edukacyjne.

Jak pogodzić rosnące wymagania w zakresie bezpieczeństwa portali publicznych z potrzebą zapewnienia dostępu do e-usług?

E-usługi dla obywateli stały się fundamentem nowoczesnego państwa. Platformy takie jak mObywatel, e-PUAP czy lokalne portale petenta ułatwiają życie milionom Polaków, lecz jednocześnie stanowią infrastrukturę krytyczną, która decyduje o ciągłości działania kraju. To sprawia, że sektor publiczny jest głównym celem zaawansowanych cyberataków. W dobie rygorystycznych wymogów dyrektywy NIS 2, ochrona tych zasobów to nie tylko obowiązek prawny, ale warunek bezpieczeństwa narodowego. W obliczu nowej ery, w której przestępcy masowo wykorzystują zagrożenia AI do automatyzacji ataków, kluczowym elementem obrony staje się ochrona przed wieloma wektorami ataków.

Odpowiedzią na te wyzwania są rozwiązania Thales (Imperva). Jako niekwestionowany lider rynku rozwiązań WAF oraz cloud WAF, systematycznie wyróżniany w raportach analitycznych Gartnera, Thales (Imperva) gwarantuje najwyższy poziom odporności cyfrowej. Platforma wykorzystuje zaawansowane AI oraz uczenie maszynowe do analizy behawioralnej w czasie rzeczywistym. Dzięki temu system natychmiast wykrywa i neutralizuje nieznane dotąd anomalie oraz ataki generowane przez sztuczną inteligencję, zanim te dotrą do infrastruktury publicznej.

Zgodnie z trendami, nowoczesna ochrona musi skutecznie odpierać ataki DDoS na warstwę aplikacji oraz sieciową, zapobiegając paraliżowi e-usług. Równie ważna jest zaawansowana ochrona przed złośliwymi botami (BOT), które za pomocą sztucznej inteligencji próbują wykradać dane lub blokować dostęp obywatelom. W dobie masowej cyfryzacji krytyczna staje się także ochrona protokołów wymiany informacji API, którymi systemy administracji przesyłają wrażliwe dane. Wdrożenie platformy przez OPTeam pozwala jednostkom publicznym skutecznie zarządzać tymi ryzykami. Cyfrowe bezpieczeństwo to proces ciągły – Thales to budowanie strategii Data Security Posture Management, która pozwala świadomie monitorować, klasyfikować i zabezpieczać dane użytkowników w każdym miejscu.

Wojciech Sawicki
Regional Sales Manager, Thales

Jak instytucje publiczne powinny podchodzić do bezpieczeństwa swoich serwisów internetowych – od wykrywania podatności, po reagowanie na incydenty?

Instytucje publiczne powinny przestać traktować cyberbezpieczeństwo jako ostatni etap projektu i zacząć budować je od pierwszego dnia powstawania systemu. Najskuteczniejszą metodą ochrony nie jest bowiem wykrywanie błędów po wdrożeniu, lecz niedopuszczanie do ich powstania. Dlatego bezpieczeństwo powinno być wbudowane w architekturę, proces wytwarzania i utrzymanie usług cyfrowych już na etapie projektowania. W praktyce oznacza to automatyczne badanie kodu źródłowego, analizę wykorzystywanych komponentów oraz skanowanie podatności przy każdej zmianie wprowadzanej do systemu. Mechanizmy te powinny działać stale i stanowić naturalny element procesu tworzenia oprogramowania, a nie dodatkową kontrolę wykonywaną tuż przed uruchomieniem usługi. Nie mniej ważne są regularne testy bezpieczeństwa prowadzone w środowiskach przedprodukcyjnych, które możliwie wiernie odwzorowują warunki produkcyjne. To właśnie tam powinny być identyfikowane błędy projektowe, podatności i nieprawidłowe konfiguracje – zanim staną się problemem obywateli lub trafią na radar cyberprzestępców.

Jednocześnie trzeba pamiętać, że cyberbezpieczeństwo nie jest projektem z datą zakończenia. To proces ciągłego doskonalenia obejmujący monitorowanie zagrożeń, zarządzanie podatnościami, aktualizację systemów oraz gotowość do reagowania na incydenty. W świecie, w którym liczba cyberataków na sektor publiczny rośnie z roku na rok, pytanie nie brzmi już „czy dojdzie do incydentu?", lecz „jak szybko go wykryjemy i ograniczymy jego skutki?" Najbardziej dojrzałe organizacje nie koncentrują się dziś na gaszeniu pożarów. Koncentrują się na takim projektowaniu i rozwijaniu usług cyfrowych, aby ryzyko wystąpienia tych pożarów było jak najmniejsze. I właśnie takie podejście powinno stać się standardem w administracji publicznej.

Dr inż. Marcin Grabarczyk
Dyrektor Pionu Transferu Technologii
i Rozwoju Biznesu, NASK

Jakie konkretne konsekwencje prawne grożą JST za niewłaściwą reakcję na incydenty w przypadku naruszeń danych i ciągłości usług?

Niezgłoszenie lub nieobsłużenie incydentów dotyczących danych i ciągłości usług lub nieusunięcie uchybień w tym zakresie będą stanowiły naruszenie znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa oraz dyrektywy NIS2. Od 03.04.2028 r. kary, które mogą być nałożone w takich sytuacjach na podmiot kluczowy (czyli np. na gminę zatrudniającą powyżej 50 osób) wynosić będą 10 mln euro lub 2% przychodów osiągniętych w roku obrotowym poprzedzającym wymierzenie kary, przy czym ma być ona nie niższa niż 20 000 zł. Z kolei dla podmiotu ważnego (np. samorządowej jednostki budżetowej) kara ma wynosić 7 mln euro lub 1,4% przychodów i być nie mniejsza niż 15 000 zł. Zgodnie z art.73a ustawy, kara może być ponadto nałożona na kierownika podmiotu w wysokości nie większej niż 100 % otrzymywanego przez niego wynagrodzenia.

Niezależnie od powyższych kar, organ właściwy do spraw cyberbezpieczeństwa, w celu przymuszenia podmiotu do wykonania jego obowiązków, może nałożyć nań w drodze decyzji okresową karę pieniężną w wysokości od 500 do 100 000 złotych za każdy dzień opóźnienia w ich realizacji.

Co istotne, jeszcze przed 03.04.2028 r. zgodnie z art. 73 ust. 5 ustawy może być zastosowana tzw. kara ekstraordynaryjna w wysokości 100 milionów złotych. Ma być ona nakładana jeżeli dojdzie do naruszenia ustawy, które spowoduje: bezpośrednie i poważne cyberzagrożenie dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi, oraz zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług publicznych.

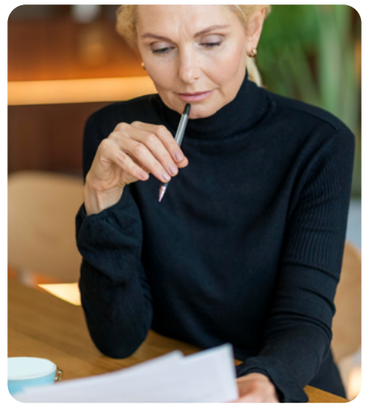
Monika Domino-Wolańczyk
Adwokat, Apogado

Dlaczego cyberbezpieczeństwo stało się dziś tematem strategicznym?

Jako były administrator systemów, który spędził lata na pierwszej linii frontu, patrzę na cyberbezpieczeństwo bez korporacyjnego lukru. Czas, gdy ochrona firmy sprowadzała się do konfiguracji firewalla i nadziei, że inżynier ma świeży backup, bezpowrotnie minął. Chmura, mikroserwisy i model rozproszony zlikwidowały pojęcie zamkniętej sieci. Dzisiejsze zagrożenia, napędzane przez grupy APT wykorzystujące sztuczną inteligencję (LLM), uderzają w całe ekosystemy i łańcuchy dostaw. Cyberbezpieczeństwo to dziś kluczowy element zarządzania ryzykiem operacyjnym i finansowym, a nie zamknięty projekt IT. Nowoczesna obrona wymaga inżynieryjnego realizmu. Standardem staje się architektura Zero Trust oraz głęboka mikrosegmentacja, które drastycznie ograniczają promień rażenia (blast radius) intruza. Przy obecnej dynamice ataków człowiek manualnie analizujący logi nie ma szans na reakcję, a sercem systemów musi być automatyzacja – zdolna do izolowania incydentów w milisekundy. Fundamentem staje się tutaj rygorystyczna dbałość o precyzyjną synchronizację czasu w całej infrastrukturze. Bez spójnej osi czasu skuteczna korelacja zdarzeń i automatyczna odpowiedź w czasie rzeczywistym są po prostu niemożliwe. Zarządy muszą zrozumieć, że stuprocentowe bezpieczeństwo to utopia. Cel przesunął się na rzecz cyber resilience (czyt. odporności cyfrowej), a miarą sukcesu nie jest brak ataków, ale zdolność organizacji do przyjęcia ciosu. Błyskawicznego ograniczenia strat w locie i sprawnego przywrócenia funkcji krytycznych. W dobie regulacji takich jak NIS2 czy DORA, dojrzałość technologiczna w obszarze security to twardy argument przewagi konkurencyjnej i przetrwanie na rynku.

Łukasz Nowatkowski
Cybersecurity Advocate & Education
Evangelist, Xopero Software

Cyfrowe usługi publiczne w praktyce. Od regulacji do realnej wartości dla urzędu i mieszkańca



Biorąc pod uwagę ilość regulacji, można by zakładać, że wdrożenia e-usług w jednostkach samorządu terytorialnego podyktowane są koniecznością prawną. W praktyce jednak wynikające z nich korzyści pokazują, że nie można ich rozpatrywać wyłącznie w kontekście obowiązków ustawowych, lecz realnych potrzeb zarówno obywateli, jak i samych instytucji publicznych.

System prawny e-usług jest już kompletny, ale i złożony. Dotyka dostępności cyfrowej, ochrony danych osobowych, cyberbezpieczeństwa, dostępu do informacji i transparentności, informatyzacji działalności oraz identyfikacji obywatela. Do tego dochodzą nowe rozporządzenia związane z AI. Wyzwaniem pozostaje więc prawidłowe i spójne przełożenie go na użyteczne doświadczenie e-usług tak obywateli, jak i pracowników instytucji.

Od cyfryzacji...

Podmioty sektora publicznego coraz lepiej odnajdują się w gąszczu przepisów i coraz lepiej rozumieją ideę cyfryzacji usług, która nie polega tylko na wdrażaniu narzędzi, ale i na projektowaniu rozwiązań z myślą o interesariuszach i usprawnieniu organizacji. Coraz rzadziej traktują ją wyłącznie jako proces informatyzacji czy projekt modernizacyjny, a częściej jako użyteczną zmianę organizacyjną.

...do korzyści

Cyfrowe usługi publiczne upraszczają procesy po stronie instytucji, a dla interesariuszy stają się łatwiejszym i bardziej dostępnym sposobem dopełnienia formalności. Z perspektywy instytucji automatyzacja procesów ogranicza ilość manualnej pracy i powtarzalnych czynności, ograniczając czas i koszty obsługi spraw, a możliwość działania zdalnego zapewnia ciągłość operacyjną. Z kolei dla interesariuszy największą korzyścią jest łatwiejszy dostęp do usług, informacji i dokumentów, uproszczenie procedur oraz przewidywalność procesu z możliwością śledzenia statusu spraw – bez konieczności wizyty w urzędzie.

3 przykłady e-usług

Wnioskowanie o udostępnianie umów zawartych przez jednostkę

Za pomocą dedykowanego rozwiązania jednostka publiczna realizuje obowiązek zapewnienia dostępu do danych publicznych dla mieszkańców, którzy mogą przeglądać repozytorium udostępnionych umów – przedmiot, kwota, data zawarcia itd. Dzięki temu pracownicy jednostki nie muszą udostępniać tych informacji metodą tradycyjną, która wymaga wizyty mieszkańca w urzędzie i bezpośredniego wglądu do kopii umowy.

Zdalny odczyt stanu wodomierzy

Radiowy odczyt pomiarów przez pracownika gminy eliminuje konieczność wchodzenia do domu, umawiania się na wizytę w przypadku nieobecności właściciela czy podawania stanu licznika telefonicznie. Dane dotyczące zużycia są automatyczne zaczytywane z kolektora do systemu, podobnie jak wyliczana opłata. Udostępniony mieszkańcom formularz na stronie WWW, umożliwia podanie stanu licznika, co jest przekazywane do systemu rozliczeniowego.

Wnioskowanie o WZ/wypis/wyrys/zaświadczenie z aktu planowania przestrzennego

Dane mieszkańca pozyskiwane są automatycznie z rejestrów państwowych już na etapie wypełniania wniosku (Węzeł Krajowy). Dzięki cyklicznej, dwukierunkowej synchronizacji danych wnioski i załączniki są automatycznie rejestrowane w EZD, a statusy spraw aktualizowane w panelu mieszkańca. Mieszkańcy mogą opłacać wnioski metodą płatności online. Eliminuje to konieczność wizyty w urzędzie, ręcznego generowania i wydruku wypisu / wyrysu dla petenta.

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.

Regulacje wyznaczają kierunek, a technologia zapewnia efekty

Prawdziwym wyzwaniem nie jest wdrożenie rozwiązania, ale przełożenie go na bezpieczną i dostępną e-usługę.

Sprawdź, jak budować realną wartość e-usług!

01. Standaryzacja i automatyzacja procesów administracyjnych.

02. Wsparcie w cyfryzacji obiegu dokumentów i zarządzaniu organizacją.

03. Usprawnienie komunikacji z mieszkańcami i interesariuszami.

04. Integracja systemów i zgodność z wymaganiami prawnymi.

05. Poprawa bezpieczeństwa i ciągłość działania instytucji.

CYFROWY
SEKTOR PUBLICZNY

http://opteam.pl/biuletyn

Wydawca:

OPTeam
EKSPERT ROZWIĄZAŃ IT

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

36-002 Jasionka
Tajęcina 113

tel. 17 867 21 00
email: opteam@opteam.pl