



PORADNIK PWCYBER

Jak ocenić realną innowacyjność i suwerenność technologiczną produktu cyberbezpieczeństwa

Przewodnik dla działów zakupowych

Opracowanie:

Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland

w ramach inicjatywy PWCyber

2026

Spis treści

Spis treści	2
Spis tabel	3
Spis rysunków.....	3
1. Wprowadzenie.....	4
2. Dlaczego ta ocena jest dziś tak trudna	5
3. Czym jest, a czym nie jest suwerenność technologiczna	6
Suwerenność pozorna a suwerenność realna	6
4. Suwerenność w dobie danych i modeli sztucznej inteligencji.....	7
5. Trzy przekonania, które warto zweryfikować	9
5.1. „Mniejszy dostawca nie udźwignie wdrożenia na skalę naszej organizacji”	9
5.2. „Nie mamy jak ocenić jakości bez uznanych certyfikatów i dużych referencji” ..	10
5.3. „Zmiana dostawcy, z którym pracujemy od lat, jest zbyt ryzykowna i kosztowna” ..	11
6. Jak oceniać realną innowacyjność produktu	12
Efekt, a nie marka	12
Weryfikacja praktyczna zamiast deklaracji	12
Zespół i kierunek rozwoju, nie tylko bieżąca wersja produktu.....	12
Elastyczność i interoperacyjność	12
Dopasowanie do lokalnego kontekstu operacyjnego.....	13
Koszt utrzymania kompetencji, nie tylko koszt zakupu	13
7. Jak oceniać realną suwerenność technologiczną dostawcy	13
Własność intelektualna	14
Lokalizacja prac rozwojowych.....	14
Jurysdykcja.....	14
Zdolność do migracji	15
Przejrzystość łańcucha dostaw technologicznych	15
Suwerenność jako stopień, nie jako stan zerojedynkowy	15
8. Jak inne kraje budują zaufanie do lokalnych technologii	16

9. Przejrzystość komponentów i łańcucha dostaw oprogramowania	17
10. Rola zamawiającego jako pierwszego klienta.....	18
11. Kryteria pozacenowe w ocenie ofert.....	19
12. Jak organizować proces zakupowy, żeby ocena była możliwa.....	20
13. Najczęstsze błędy przy ocenie innowacyjnych rozwiązań	21
14. Jak czytać deklaracje i materiały marketingowe dostawców	22
15. Zależność od dostawcy jako ryzyko do zarządzania.....	23
Struktura własnościowa i ryzyko przejęcia.....	24
16. Jak zacząć	24
17. Podsumowanie	25
18. Słownik pojęć	27
19. O klastrze CyberMadeInPoland	28

Spis tabel

Tabela 1: Suwerenność pozorna a suwerenność realna – porównanie na czterech wymiarach	7
--	---

Spis rysunków

Rysunek 1: Pięć wymiarów oceny suwerenności technologicznej dostawcy.....	14
--	----

1. Wprowadzenie

Działy zakupowe administracji publicznej, spółek Skarbu Państwa i podmiotów regulowanych stoją dziś przed zadaniem, które jeszcze dekadę temu miało znacznie prostszy wymiar. Wybór dostawcy rozwiązania cyberbezpieczeństwa nie sprowadza się już wyłącznie do porównania funkcjonalności i ceny. Coraz częściej pojawia się pytanie o coś trudniejszego do zmierzenia: czy wybrane rozwiązanie rzeczywiście wzmacnia odporność organizacji w długim horyzoncie, czy tylko przenosi ryzyko w inne miejsce – do zależności od jednego dostawcy, jednej jurysdykcji, jednego modelu licencyjnego.

Ustawa o krajowym systemie cyberbezpieczeństwa, implementująca dyrektywę NIS2, wprowadza obowiązek zarządzania ryzykiem w łańcuchu dostaw. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029 po raz pierwszy wprost wskazuje stymulowanie krajowego rynku cyberbezpieczeństwa jako jeden z kierunków strategicznych państwa. Polityka Zakupowa Państwa na lata 2026–2029 wprowadza mechanizmy, które mają umożliwić uwzględnianie w postępowaniach kryteriów jakościowych, innowacyjnych i związanych z odpornością, a nie tylko ceny. Wszystkie te dokumenty wskazują ten sam kierunek, ale żaden z nich nie odpowiada wprost na pytanie praktyczne, które codziennie stoi przed osobą przygotowującą opis przedmiotu zamówienia: **jak w praktyce ocenić, czy oferowane rozwiązanie jest rzeczywiście innowacyjne i czy jego zastosowanie realnie zwiększa niezależność technologiczną organizacji**, a nie jedynie deklaruje ją w materiałach marketingowych.

Ten poradnik nie jest namową do preferowania polskich rozwiązań kosztem jakości czy bezpieczeństwa. Jest próbą odpowiedzi na inne pytanie: **jakimi kryteriami posługiwać się, żeby ocena innowacyjności i suwerenności technologicznej produktu cyberbezpieczeństwa była rzetelna, niezależna od marki i możliwa do obronienia** – niezależnie od tego, czy ostatecznie wybranym dostawcą będzie firma polska, europejska czy globalna.

Adresatami poradnika są przede wszystkim osoby odpowiedzialne za przygotowanie opisu przedmiotu zamówienia, oceniające oferty oraz podejmujące decyzje o wyborze technologii w administracji publicznej, spółkach Skarbu Państwa oraz podmiotach kluczowych i ważnych w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa. Materiał może być również przydatny dla dostawców rozwiązań, którzy chcą rozumieć, jakie pytania powinni być gotowi zadać sobie sami, zanim zaczną odpowiadać na pytania zamawiającego.

Poradnik celowo nie zajmuje się szczegółową interpretacją przepisów prawa zamówień publicznych ani orzecznictwem w tym zakresie – to materia wymagająca

odrębnego, prawniczego opracowania, do którego przygotowania zachęcamy instytucje dysponujące odpowiednim zapleczem prawnym. Skupiamy się tu na warstwie merytorycznej i organizacyjnej: na pytaniach, jakie warto sobie zadać, i na sposobie myślenia o produkcie i dostawcy, niezależnie od tego, w jakiej formie prawnej zostanie ostatecznie przeprowadzone postępowanie. Uważamy, że to właśnie na tym poziomie – zanim jeszcze dojdzie do sformułowania konkretnych zapisów specyfikacji – najczęściej rozstrzyga się, czy ocena innowacyjnego rozwiązania będzie rzetelna, czy pozorna.

2. Dlaczego ta ocena jest dziś tak trudna

Polski rynek IT rośnie dynamicznie, ale struktura tego wzrostu nie sprzyja łatwej ocenie lokalnych, innowacyjnych rozwiązań. Import produktów cyfrowych odpowiada za większość wartości krajowego rynku IT, a wśród pięćdziesięciu największych firm branży w zestawieniach rynkowych jedynie nieliczne można uznać za podmioty z polskim kapitałem i polską własnością intelektualną. **W efekcie osoba przygotowująca opis przedmiotu zamówienia w naturalny sposób styka się przede wszystkim z ofertą globalnych producentów – są lepiej widoczne w kanałach dystrybucji, częściej obecne na konferencjach branżowych, lepiej opisane w materiałach analitycznych.**

Dodatkowym czynnikiem jest struktura postępowań przetargowych w obszarze IT. W Polsce znaczący odsetek postępowań kończy się złożeniem jednej oferty, co wskazuje, że opis przedmiotu zamówienia bywa formułowany w sposób, który – często nieświadomie – zawęża krąg potencjalnych wykonawców do jednego, znanego już zamawiającemu dostawcy. Nie musi to wynikać ze złej woli. Znacznie częściej jest efektem naturalnego mechanizmu: łatwiej opisać wymagania, odwołując się do rozwiązania, które się zna i z którym ma się dobre doświadczenia, niż zbudować opis od podstaw, w oderwaniu od konkretnej marki.

Ten kontekst tłumaczy, dlaczego ocena innowacyjnych, mniej rozpoznawalnych rozwiązań wymaga dziś świadomego wysiłku metodycznego, a nie tylko dobrej woli. Kolejne rozdziały proponują konkretne sposoby, jak ten wysiłek zorganizować.

Warto też zwrócić uwagę na jeszcze jedną prawidłowość: struktura zatrudnienia i inwestycji w rozwój produktu wygląda zupełnie inaczej u dystrybutora czy integratora niż u rzeczywistego producenta technologii. Duża część kadr zatrudnionych po stronie globalnych dostawców obecnych na polskim rynku pracuje w sprzedaży, wsparciu wdrożeniowym i marketingu, podczas gdy prace rozwojowe nad samym produktem toczą się poza Polską. Dla porównania, w mniejszych,

krajowych firmach technologicznych relacja ta bywa odwrócona – większość zespołu stanowią inżynierowie odpowiedzialni bezpośrednio za rozwój produktu. Ta różnica ma praktyczne znaczenie dla zamawiającego: określa, z kim faktycznie rozmawia w trakcie wdrożenia i kto ma realny wpływ na to, czy zgłoszony problem zostanie rozwiązany szybko, czy trafi do kolejki zgłoszeń w centrali odległej o tysiące kilometrów.

3. Czym jest, a czym nie jest suwerenność technologiczna

Pojęcie suwerenności technologicznej pojawia się dziś w niemal każdej debacie o cyberbezpieczeństwie, ale rzadko jest precyzyjnie definiowane. To utrudnia jego praktyczne zastosowanie w ocenie ofert – trudno ocenić coś, czego nie da się jednoznacznie opisać.

Na potrzeby oceny produktów i usług cyberbezpieczeństwa warto przyjąć definicję operacyjną: **suwerenność technologiczna to zdolność organizacji do świadomego kontrolowania, rozwijania i bezpiecznego utrzymywania kluczowych systemów cyfrowych, przy zachowaniu realnej możliwości działania i zmiany dostawcy w sytuacji kryzysowej, geopolitycznej lub rynkowej – bez paraliżu operacyjnego.**

Rozumiana w ten sposób suwerenność technologiczna nie oznacza rezygnacji ze współpracy z dostawcami globalnymi ani dążenia do pełnej samowystarczalności. Nie jest tożsama z lokalizacją danych – fizyczna obecność danych na terenie Polski niczego nie gwarantuje, jeśli kontrola nad kodem, kluczami bezpieczeństwa, architekturą systemu czy kierunkiem jego rozwoju pozostaje poza zasięgiem organizacji. Nie jest też prostym preferowaniem kapitału deklaratorywnie polskiego, bez analizy tego, gdzie faktycznie powstaje własność intelektualna i kto podejmuje decyzje o rozwoju produktu.

Suwerenność pozorna a suwerenność realna

Warto rozróżniać sygnały, które sprawiają wrażenie niezależności technologicznej, od cech, które rzeczywiście tę niezależność zapewniają. Poniższe zestawienie pokazuje tę różnicę na czterech wymiarach, które najczęściej bywają mylone.

Tabela 1: Suwerenność pozorna a suwerenność realna – porównanie na czterech wymiarach

Wymiar	Sygnał pozorny	Rzeczywisty wskaźnik
Lokalizacja danych	Dane fizycznie przechowywane na terenie Polski (data residency)	Dane pod wyłączną kontrolą prawną i operacyjną organizacji, niezależnie od lokalizacji serwera
Technologia	Zamknięty stos technologiczny licencjonowany od jednego, zagranicznego dostawcy	Otwarte standardy, udokumentowane API, możliwość integracji z innymi systemami
Zależność	Deklaracja niezależności w materiałach marketingowych	Realna, zweryfikowana możliwość migracji do innego rozwiązania bez paraliżu operacyjnego
Rola dostawcy	Reseller lub lokalny partner wdrożeniowy globalnej platformy	Twórca i właściciel własności intelektualnej rozwiązania, z realną kontrolą nad jego rozwojem

Tekst alternatywny: Tabela porównuje cztery wymiary suwerenności technologicznej (lokalizacja danych, technologia, zależność, rola dostawcy), zestawiając dla każdego z nich sygnał pozorny z rzeczywistym, sprawdzalnym wskaźnikiem.

W praktyce ocena suwerenności technologicznej produktu sprowadza się do kilku pytań, które można zadać niezależnie od tego, skąd pochodzi dostawca: **kto ma kontrolę nad własnością intelektualną rozwiązania, gdzie faktycznie prowadzone są prace rozwojowe, jakiej jurysdykcji podlega dostawca i jego dane, na ile organizacja zachowuje zdolność do migracji lub zmiany dostawcy bez nieproporcjonalnych kosztów, oraz na ile architektura rozwiązania jest interoperacyjna i oparta na otwartych standardach, a nie na zamkniętym ekosystemie jednego producenta.**

Warto podkreślić: te same pytania należy zadawać każdemu dostawcy – również polskiemu. Sama rejestracja spółki w Polsce nie jest równoznaczna z suwerennością, jeśli produkt bazuje na licencjonowanej technologii zagranicznej, a kluczowe decyzje rozwojowe zapadają poza krajem. **Traktowanie tych pytań jako uniwersalnego kryterium oceny, a nie jako filtra narodowościowego, jest tym, co odróżnia rzetelną ocenę suwerenności technologicznej od protekcjonizmu.**

4. Suwerenność w dobie danych i modeli sztucznej inteligencji

Coraz większa część innowacji w cyberbezpieczeństwie opiera się dziś na mechanizmach uczenia maszynowego i modelach sztucznej inteligencji między innymi

w wykrywaniu anomalii, analizie zagrożeń, automatyzacji reakcji na incydenty czy ocenie ryzyka. To dodaje nowy, ważny wymiar do oceny suwerenności technologicznej, który warto rozpatrywać osobno od pytań o kod źródłowy czy architekturę systemu.

Pierwsze pytanie dotyczy tego, gdzie i na jakich danych trenowany jest model wykorzystywany przez rozwiązanie. Model trenowany głównie na danych pochodzących z jednego regionu świata może gorzej rozpoznawać wzorce charakterystyczne dla lokalnego kontekstu zagrożeń – w tym ataki prowadzone w języku polskim czy wymierzone specyficznie w polskie instytucje. Warto pytać dostawcę wprost, jak wygląda proces trenowania i dostrajania modelu oraz czy istnieje możliwość jego lokalnego dostrajania w oparciu o dane organizacji, bez konieczności przesyłania tych danych poza jej infrastrukturę.

Drugie pytanie dotyczy przepływu danych. Rozwiązania oparte na modelach chmurowych często wymagają przesyłania danych operacyjnych – logów, ruchu sieciowego, próbek złośliwego oprogramowania – do infrastruktury dostawcy w celu analizy. Warto rozumieć, gdzie fizycznie te dane trafiają, jak długo są przechowywane, czy są wykorzystywane do dalszego trenowania modeli współdzielonych z innymi klientami dostawcy oraz jaka jurysdykcja obejmuje ten proces. To pytanie ma szczególne znaczenie w przypadku danych wrażliwych lub dotyczących infrastruktury krytycznej.

Trzecie pytanie dotyczy wyjaśnialności działania modelu. Systemy oparte na sztucznej inteligencji, które podejmują lub rekomendują decyzje istotne dla bezpieczeństwa organizacji, powinny umożliwiać zrozumienie, dlaczego dany wniosek został wyciągnięty – nie tylko sam wynik, ale i jego uzasadnienie. Rozwiązanie działające jako całkowicie zamknięta „czarna skrzynka” utrudnia audyt, weryfikację błędów i budowanie zaufania zespołu bezpieczeństwa do rekomendacji systemu, niezależnie od tego, jak dokładny jest sam model.

Warto też pamiętać, że rosnące wykorzystanie sztucznej inteligencji w cyberbezpieczeństwie podlega dziś dodatkowo regulacjom unijnym dotyczącym systemów sztucznej inteligencji. Ocena zgodności rozwiązania z tymi wymaganiami – w zakresie, w jakim mają zastosowanie do danego przypadku użycia – staje się kolejnym, praktycznym elementem oceny dojrzałości i wiarygodności dostawcy, niezależnie od tego, skąd pochodzi.

Wymiar ten warto też odnieść z powrotem do samej innowacyjności rozwiązania.

Dostawca, który potrafi jasno i konkretnie odpowiedzieć na pytania o pochodzenie danych treningowych, mechanizm dostrajania modelu do lokalnego kontekstu oraz sposób wyjaśniania jego decyzji, zwykle reprezentuje wyższy poziom dojrzałości

inżynierskiej niż dostawca ograniczający się do ogólnego stwierdzenia, że produkt „wykorzystuje sztuczną inteligencję”. Konkretność odpowiedzi na te pytania jest w praktyce jednym z najlepszych dostępnych dziś testów odróżniających rzeczywistą innowacyjność od jej deklaracji.

5. Trzy przekonania, które warto zweryfikować

W rozmowach z działami zakupowymi powtarzają się trzy przekonania, które w praktyce utrudniają rzetelną ocenę innowacyjnych rozwiązań, niezależnie od intencji osoby przygotowującej postępowanie. Warto przyjrzeć się każdemu z nich osobno - nie po to, by je odrzucić, ale by zrozumieć, kiedy są uzasadnione, a kiedy prowadzą do błędnych wniosków.

5.1. „Mniejszy dostawca nie udźwignie wdrożenia na skalę naszej organizacji”.

To przekonanie miesza dwie różne rzeczy: wielkość firmy dostawcy oraz skalowalność jej produktu. Są to cechy od siebie niezależne. Wiele nowoczesnych rozwiązań cyberbezpieczeństwa, zwłaszcza tych budowanych w architekturze chmurowej, kontenerowej czy opartych na otwartym kodzie, skaluje się w sposób niezależny od liczby pracowników zatrudnionych u producenta. O zdolności produktu do obsługi dużej organizacji świadczy architektura systemu, a nie wielkość zespołu sprzedażowego czy rozpoznawalność marki.

Dobłą praktyką jest oddzielenie w ocenie tych dwóch wymiarów. **Skalowalność produktu warto weryfikować bezpośrednio – poprzez test w środowisku zbliżonym do docelowego, analizę architektury rozwiązania oraz rozmowę techniczną z zespołem inżynierskim dostawcy, a nie z działem sprzedaży.** Stabilność i zdolność do długoterminowego wsparcia produktu to osobne pytanie, dla którego pomocne bywają wskaźniki finansowe dostawcy czy historia rozwoju produktu, ale nie musi to być pytanie rozstrzygane wyłącznie przez wielkość organizacji dostawcy.

Warto też pamiętać, że mniejszy, wyspecjalizowany dostawca bywa w praktyce bardziej elastyczny w dostosowaniu produktu do specyficznych potrzeb organizacji niż globalny producent, dla którego pojedynczy kontrakt w Polsce stanowi ułamek procenta globalnych przychodów i rzadko wpływa na priorytety rozwoju produktu.

Pomocnym ćwiczeniem jest odwrócenie pytania: zamiast pytać, czy dostawca jest wystarczająco duży, warto zapytać, co konkretnie w tej organizacji miałyby zawieść przy większej skali – czy to przepustowość systemu, dostępność wsparcia

technicznego w określonych godzinach, czy zdolność do jednoczesnej obsługi wielu lokalizacji. Każdy z tych elementów da się sprawdzić bezpośrednio, w oderwaniu od wielkości firmy dostawcy, a odpowiedź na tak postawione pytanie jest zwykle znacznie bardziej użyteczna niż ogólne przekonanie o barierze skali.

5.2. „Nie mamy jak ocenić jakości bez uznanych certyfikatów i dużych referencji”

Certyfikaty i referencje są użytecznym, ale niepełnym źródłem informacji o jakości rozwiązania. Problem pojawia się wtedy, gdy stają się jedynym dopuszczalnym dowodem – bo wtedy w naturalny sposób premiują dostawców, którzy już wcześniej mieli dostęp do dużych kontraktów, niezależnie od aktualnej jakości technicznej ich produktu. **To mechanizm samowzmacniający się: duże referencje ułatwiają zdobycie kolejnych dużych referencji, a ich brak nawet przy doskonałym produkcie, skutecznie wyklucza z udziału w kolejnych postępowaniach.**

Dobłą praktyką jest traktowanie referencji jako jednego z kilku równorzędnych źródeł dowodu, obok bezpośredniej weryfikacji technicznej. **Certyfikaty branżowe o jednoznacznym, mierzalnym znaczeniu – takie jak ISO 27001 czy certyfikaty zgodności z konkretnymi normami technicznymi – warto traktować inaczej niż komercyjne rankingi i zestawienia analityczne, które, niezależnie od swojej użyteczności informacyjnej, powstają w oparciu o metodologię nastawioną na globalną skalę rynku i rzadko uwzględniają specyfikę pojedynczego, lokalnego wdrożenia.**

Najbardziej wiarygodnym uzupełnieniem referencji jest bezpośrednia weryfikacja: **test rozwiązania w środowisku zbliżonym do docelowego, rozmowa z zespołem technicznym dostawcy, analiza dokumentacji architektury i modelu bezpieczeństwa, a w przypadku rozwiązań opartych na otwartym kodzie – możliwość przeglądu samego kodu źródłowego.** Żadne oświadczenie producenta o zgodności z wymaganiami nie zastąpi takiej weryfikacji i to niezależnie od tego, czy oświadczenie składa duża, czy mała firma.

Warto też odróżniać referencje ilościowe od referencji jakościowych. Informacja, że rozwiązanie wdrożono u stu klientów, mówi niewiele o tym, czy sprawdza się ono w kontekście zbliżonym do sytuacji danej organizacji. Znacznie bardziej wartościowa jest pojedyncza, dobrze udokumentowana referencja z organizacji o podobnej skali, branży lub profilu ryzyka – nawet jeśli dostawca dysponuje ich niewieloma. To jakość dopasowania referencji, a nie ich liczba, powinna być głównym kryterium oceny.

5.3. „Zmiana dostawcy, z którym pracujemy od lat, jest zbyt ryzykowna i kosztowna”

To przekonanie jest najbardziej racjonalne z trzech opisanych tutaj – i dlatego najtrudniej się z nim zmierzyć. Rzeczywiście, zmiana sprawdzonego rozwiązania niesie ryzyko operacyjne, a zespół przyzwyczajony do jednego narzędzia potrzebuje czasu na naukę nowego. **Problem pojawia się wtedy, gdy ten realny koszt zmiany nie jest w ogóle liczony i porównywany z równie realnym, choć mniej widocznym, kosztem trwania w zależności od jednego dostawcy.**

Dobłą praktyką jest liczenie całkowitego kosztu posiadania (TCO) w dłuższym horyzoncie – pięciu, ośmiu lat – a nie tylko kosztu wdrożenia. W taki rachunek warto włączyć nie tylko licencję i utrzymanie, ale też koszt potencjalnej migracji w przyszłości, ryzyko zmiany warunków licencyjnych przez dostawcę w sytuacji braku realnej alternatywy po stronie zamawiającego, oraz wartość zachowania zdolności negocjacyjnej. Organizacja, która ma wiarygodną alternatywę, negocjuje z pozycji siły, a nie z pozycji zakładnika.

Zmiana dostawcy nie musi być rewolucją. Dobłą praktyką jest podejście stopniowe: równoległe testowanie nowego rozwiązania obok istniejącego, w wybranym, ograniczonym obszarze działalności organizacji, zanim zapadnie decyzja o pełnej migracji. Taki model – wykorzystanie istniejącego rozwiązania jako punktu odniesienia i stopniowe budowanie doświadczenia z alternatywą – pozwala ograniczyć ryzyko operacyjne przy jednoczesnym budowaniu realnej zdolności wyboru w przyszłości. Warto też rozważyć mechanizmy kontraktowe ograniczające ryzyko zależności od pojedynczego dostawcy niezależnie od jego wielkości na przykład zobowiązanie do deponowania kodu źródłowego u zaufanej trzeciej strony, które zabezpiecza organizację na wypadek zaprzestania działalności przez dostawcę (tzw. Software escrow).

Warto też odróżnić przyzwyczajenie zespołu od realnej przewagi technicznej rozwiązania – to dwa różne argumenty za utrzymaniem status quo, które łatwo ze sobą pomylić. Przyzwyczajenie jest kosztem jednorazowym, możliwym do zamortyzowania poprzez szkolenie i stopniowe wdrożenie. Realna przewaga techniczna jest argumentem trwałym, ale wymaga potwierdzenia w bezpośrednim porównaniu, a nie samego stwierdzenia, że dotychczasowe rozwiązanie „zawsze działało dobrze”. Oddzielenie tych dwóch wątków w dyskusji wewnątrz organizacji pozwala podjąć decyzję opartą na faktach, a nie wyłącznie na sile przyzwyczajenia.

6. Jak oceniać realną innowacyjność produktu

Ocena innowacyjności produktu cyberbezpieczeństwa bywa trudna, bo samo to słowo jest pojemne i łatwo nadużywane w materiałach marketingowych każdego dostawcy. Poniżej zaprezentowano kilka wymiarów, które w praktyce pozwalają odróżnić innowacyjność rzeczywistą od deklarowanej.

Efekt, a nie marka

Najbardziej wiarygodną metodą oceny jest zdefiniowanie pożądanego efektu – konkretnego problemu, który rozwiązanie ma rozwiązać, oraz mierzalnych parametrów technicznych – a następnie sprawdzenie, czy oferowany produkt rzeczywiście ten efekt osiąga, niezależnie od tego, jaką technologię czy architekturę wykorzystuje. **Opis przedmiotu zamówienia skoncentrowany na efekcie, a nie na konkretnej technologii czy marce, w naturalny sposób otwiera pole do oceny produktów, które osiągają ten sam cel w inny, czasem bardziej nowoczesny sposób.**

Weryfikacja praktyczna zamiast deklaracji

Bezpośrednia weryfikacja działania rozwiązania w warunkach zbliżonych do docelowych – test typu proof of concept – ma zupełnie inną wartość dowodową niż deklaracja producenta, że rozwiązanie spełnia dane wymaganie. Warto, aby taki test był standardowym, a nie wyjątkowym elementem procesu oceny, szczególnie w przypadku rozwiązań planowanych do zastosowania w obszarach o podwyższonym znaczeniu dla ciągłości działania organizacji.

Zespół i kierunek rozwoju, nie tylko bieżąca wersja produktu

Rozmowa z zespołem inżynierskim dostawcy – nie tylko z działem sprzedaży – pozwala zrozumieć, w jakim kierunku rozwija się rozwiązanie, jak często i w jaki sposób reaguje na nowe zagrożenia, jak wygląda proces zarządzania podatnościami itp. **Produkt innowacyjny to nie tylko produkt nowoczesny w chwili zakupu, ale produkt rozwijany w sposób, który pozwala mu pozostać aktualnym w horyzoncie kilku lat.**

Elastyczność i interoperacyjność

Rozwiązanie zaprojektowane w oparciu o otwarte standardy, z udokumentowanym interfejsem programistycznym i możliwością integracji z innymi systemami, daje organizacji większą swobodę w budowaniu architektury bezpieczeństwa niż

rozwiązanie zamknięte, wymuszające pełne przejście na ekosystem jednego producenta. Ten wymiar jest szczególnie istotny w kontekście oceny innowacyjności, bo produkty budowane od podstaw w ostatnich latach – co dotyczy wielu mniejszych, dynamicznie rozwijających się firm – częściej wykorzystują nowoczesne, otwarte architektury niż rozwiązania rozwijane przez dekady w dużych organizacjach, gdzie zmiana fundamentalnej architektury wiąże się z ogromnym kosztem.

Dopasowanie do lokalnego kontekstu operacyjnego

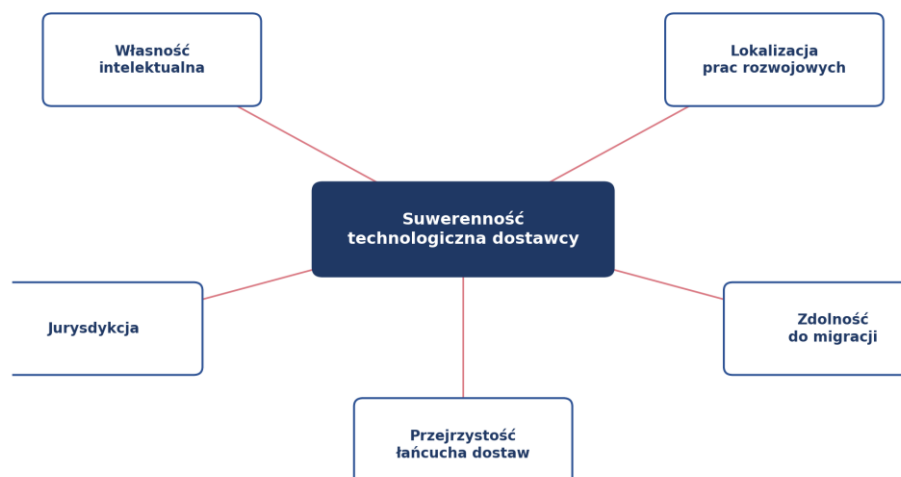
W obszarze cyberbezpieczeństwa, zwłaszcza w zakresie analizy zagrożeń, wykrywania oszustw czy zarządzania tożsamością, produkt zbudowany z uwzględnieniem lokalnej specyfiki, języka i wzorców ataków charakterystycznych dla danego regionu może w praktyce działać skuteczniej niż globalne rozwiązanie zbudowane na uśrednionych, światowych wzorcach, nawet jeśli to drugie dysponuje większą bazą danych historycznych. Warto pytać nie tylko o skalę zgromadzonych danych, ale o ich trafność i aktualność w kontekście realnych zagrożeń, z którymi mierzy się organizacja.

Koszt utrzymania kompetencji, nie tylko koszt zakupu

Innowacyjność rozwiązania warto oceniać także przez pryzmat tego, ile wysiłku organizacja będzie musiała włożyć w utrzymanie kompetencji potrzebnych do jego obsługi. Rozwiązanie wymagające wąskiej, trudno dostępnej na rynku pracy specjalizacji stwarza ryzyko operacyjne niezależne od jakości samego produktu – wystarczy odejście jednej kluczowej osoby z zespołu, żeby organizacja utraciła zdolność efektywnego korzystania z systemu. Warto pytać dostawcę o to, jak wygląda typowa ścieżka wdrożenia nowego członka zespołu do pracy z rozwiązaniem, jakie materiały szkoleniowe i jaki poziom wsparcia oferuje w tym zakresie, oraz czy interfejs i dokumentacja są zaprojektowane z myślą o realnym, samodzielny użytkowaniu przez zespół zamawiającego, a nie wyłącznie o pracy wspólnie z konsultantami dostawcy.

7. Jak oceniać realną suwerenność technologiczną dostawcy

Jeśli suwerenność technologiczna rozumiana jest jako zdolność do zachowania kontroli i możliwości wyboru, jej ocena wymaga spojrzenia wykraczającego poza kraj rejestracji spółki. Poniżej kilka pytań, które warto zadać niezależnie od pochodzenia dostawcy.



Rysunek 1: Pięć wymiarów oceny suwerenności technologicznej dostawcy

Tekst alternatywny: Diagram przedstawia pięć wymiarów oceny suwerenności technologicznej dostawcy, połączonych z centralnym pojęciem suwerenności: własność intelektualna, lokalizacja prac rozwojowych, jurysdykcja, zdolność do migracji oraz przejrzystość łańcucha dostaw. Każdy wymiar jest omówiony osobno w dalszej części rozdziału.

Własność intelektualna

Czy dostawca jest twórcą i właścicielem kodu oraz architektury rozwiązania, czy pełni raczej rolę dystrybutora bądź integratora technologii licencjonowanej od podmiotu trzeciego? **Odpowiedź na to pytanie determinuje, kto faktycznie decyduje o kierunku rozwoju produktu i kto ponosi odpowiedzialność za jego bezpieczeństwo w długim horyzoncie.** Warto pytać wprost, a nie zakładać odpowiedzi na podstawie samej nazwy firmy czy kraju jej rejestracji.

Lokalizacja prac rozwojowych

Gdzie faktycznie pracuje zespół inżynierski odpowiedzialny za rozwój produktu? Czy organizacja ma możliwość bezpośredniego kontaktu z osobami odpowiedzialnymi za architekturę i bezpieczeństwo rozwiązania, czy komunikacja odbywa się wyłącznie przez warstwy pośrednie – lokalnego partnera handlowego, regionalne biuro wsparcia? **Bliskość zespołu rozwojowego przekłada się bezpośrednio na czas reakcji na zgłoszone problemy oraz na możliwość wpływania na priorytety rozwoju produktu.**

Jurysdykcja

Jakiemu prawu podlega dostawca i jego ewentualni podwykonawcy, gdzie fizycznie przechowywane i przetwarzane są dane, oraz czy istnieje ryzyko, że decyzje

regulacyjne lub polityczne podjęte poza Unią Europejską mogą wpłynąć na dostępność lub integralność wykorzystywanego rozwiązania. To pytanie ma szczególne znaczenie dla systemów przetwarzających dane wrażliwe lub wspierających procesy o znaczeniu krytycznym dla ciągłości działania organizacji.

Zdolność do migracji

Co będzie się działo, jeśli za pięć lat organizacja zdecyduje się na zmianę dostawcy albo dostawca wstrzyma działalność? Czy dane i konfiguracje są przenaszalne do innego systemu, czy architektura rozwiązania wymusza głęboką integrację uniemożliwiającą realną zmianę bez pełnej przebudowy infrastruktury? **Dobłą praktyką jest weryfikowanie tej zdolności już na etapie wyboru dostawcy, a nie dopiero w momencie, gdy migracja staje się konieczna.**

Przejrzystość łańcucha dostaw technologicznych

Wielu dostawców, niezależnie od skali, korzysta z komponentów, bibliotek czy usług chmurowych podmiotów trzecich. Rzetelna ocena suwerenności technologicznej wymaga zrozumienia, gdzie w tym łańcuchu znajdują się rzeczywiste punkty zależności – nie wystarczy ocenić samego dostawcy pierwszego kontaktu, jeśli kluczowa część rozwiązania działa na infrastrukturze lub komponentach podmiotu spoza Unii Europejskiej.

Żadne z powyższych pytań nie jest pytaniem o narodowość dostawcy. Są to pytania o strukturę kontroli, które pozwalają ocenić realne ryzyko zależności technologicznej – niezależnie od tego, czy odpowiedzi wypadają korzystnie dla dostawcy polskiego, europejskiego czy globalnego. Konsekwentne, niewybiórcze stosowanie tych pytań wobec każdej oferty jest tym, co odróżnia rzetelną politykę zakupową od działania doraźnego.

Suwerenność jako stopień, nie jako stan zerojedynekowy

Warto na koniec podkreślić, że żadne rozwiązanie, niezależnie od pochodzenia, nie jest w pełni suwerenne w sensie absolutnym. Nawet produkt zbudowany od podstaw przez polski zespół zwykle korzysta z pewnych komponentów zewnętrznych: bibliotek programistycznych, usług chmurowych, sprzętu sieciowego. Traktowanie suwerenności technologicznej jako stanu zerojedynekowego – „mamy ją” albo „jej nie mamy” – prowadzi do nieproduktywnych dyskusji i łatwo daje się zdyskredytować przykładem jednego zależnego komponentu.

Bardziej użyteczne jest myślenie o suwerenności jako o stopniu, który różni się w zależności od tego, którego z opisanych wcześniej wymiarów dotyczy – własności

intelektualnej, lokalizacji rozwoju, jurysdykcji, zdolności do migracji, przejrzystości łańcucha dostaw. **Rozwiązanie może być bardzo suwerenne w jednym wymiarze, a jednocześnie zależne w innym – i to jest normalna, akceptowalna sytuacja, o ile organizacja ma tego świadomość i świadomie zarządza wynikającym z niej ryzykiem, zamiast zakładać pełną niezależność tam, gdzie jej w rzeczywistości nie ma.**

8. Jak inne kraje budują zaufanie do lokalnych technologii

Problem oceny nowych, mniej rozpoznawalnych dostawców rozwiązań cyberbezpieczeństwa jest widoczny nie tylko w Polsce. Kilka krajów, które świadomie postawiły na rozwój krajowego sektora cyberbezpieczeństwa, wypracowało mechanizmy ułatwiające zamawiającym ocenę wiarygodności lokalnych rozwiązań, bez rezygnowania z konkurencyjności rynku.

We Francji francuska agencja bezpieczeństwa systemów informacyjnych ANSSI prowadziła program certyfikacji znany jako *Visa de sécurité*, w ramach którego rozwiązania przechodzą niezależny, państwowy audyt bezpieczeństwa. Uzyskanie takiej certyfikacji nie jest barierą wejścia na rynek, lecz uproszczonym, wiarygodnym sygnałem jakości. Dla zamawiającego oznacza to możliwość oparcia się na jednym, zaufanym źródle oceny, zamiast przeprowadzania pełnej weryfikacji technicznej za każdym razem od podstaw. W Singapurze podobną funkcję pełni system oceny bezpieczeństwa produktów prowadzony przez Cyber Security Agency of Singapore, przedstawiający poziom bezpieczeństwa rozwiązań w przystępnej, zrozumiałej dla zamawiającego skali.

Warto też zwrócić uwagę na Izrael i Estonię – dwa mniejsze kraje, które mimo ograniczonej wielkości rynku wewnętrznego zbudowały rozpoznawalne, konkurencyjne na skalę globalną sektory cyberbezpieczeństwa. W obu przypadkach istotną rolę odegrało świadome wykorzystanie sektora publicznego jako pierwszego, wymagającego klienta oraz bliska współpraca między instytucjami odpowiedzialnymi za bezpieczeństwo państwa a rodzimymi firmami technologicznymi już na wczesnym etapie rozwoju produktu. To potwierdza obserwację z wcześniejszego rozdziału tego poradnika: **rola zamawiającego publicznego jako pierwszego klienta nie jest tylko postulatem, ale sprawdzonym, powtarzalnym elementem budowy dojrzałego, konkurencyjnego sektora technologicznego.**

Wspólnym mianownikiem tych rozwiązań jest to, że nie zastępują one oceny merytorycznej, lecz ją ułatwiają: dają zamawiającemu punkt odniesienia niezależny od komercyjnych rankingów tworzonych przez prywatne firmy analityczne, a jednocześnie dostępny również dla mniejszych, lokalnych dostawców, dla których

udział w kosztownych, globalnych programach certyfikacyjnych bywa barierą nie do pokonania. Polska nie dysponuje dziś gotowym, jednolitym narzędziem oceny tego typu, ale kierunek wyznaczony w obu dokumentach strategicznych jest wyraźny. Polityka Zakupowa Państwa zapowiada tworzenie – poprzez zamówienia publiczne – „pierwszych rynków zbytu dla kluczowych innowacyjnych produktów i usług” (Priorytet I, Cel działania 3¹) oraz „opracowanie katalogu kryteriów oceny poziomu suwerenności produktów i usług ICT (Cel działania 5²).” Strategia Cyberbezpieczeństwa RP przewiduje z kolei ułatwienia zakupowe, pilotażowe wdrożenia w instytucjach publicznych i wsparcie certyfikacyjne dla rozwiązań krajowych producentów (cel szczegółowy 4, pkt 8.1³) oraz rozwija współpracę publiczno-prywatną (pkt 7.6, program PWCyber⁴) w tym wprost wskazuje Celu szczegółowy 4 - Zwiększanie potencjału krajowej bazy technologiczno-przemysłowej oraz wzmocnienie suwerenności technologicznej Rzeczypospolitej Polskiej w tym obszarze za jeden z priorytetów⁵. Oba dokumenty traktują rozwój rynku, współpracę na linii biznes–państwo i suwerenność technologiczną jako istotne funkcje zamówień publicznych – zbliżając się do modelu, w którym państwo pełni rolę pierwszego, kotwiczącego odbiorcy (anchor tenant).

9. Przejrzystość komponentów i łańcucha dostaw oprogramowania

Innowacyjność i suwerenność technologiczna produktu zależą nie tylko od tego, kto go tworzy, ale też z czego jest zbudowany. Współczesne oprogramowanie niezależnie od tego, czy powstaje w Polsce, czy za granicą, niemal zawsze korzysta z bibliotek

¹ Polityka zakupowa państwa na lata 2026–2029, Priorytet I „Budowanie konkurencyjności i potencjału polskiej gospodarki”, Cel działania 3 „Promowanie zamówień publicznych na innowacje”, (cyt.: „(...) państwo będzie dążyć do tworzenia, poprzez zamówienia publiczne, pierwszych rynków zbytu dla kluczowych innowacyjnych produktów i usług”).

² Tamże, Priorytet I, Cel działania 5 „Cyberbezpieczeństwo i ochrona danych w zamówieniach publicznych”, Wytyczne dla instytucji wspierających wdrożenie Polityki, (zapowiedź stworzenia „katalogu kryteriów oceny poziomu suwerenności zamawianych produktów i usług ICT”).

³ Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej, stanowiąca załącznik do uchwały nr 92 Rady Ministrów z dnia 10 marca 2026 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej cel szczegółowy 4, pkt 8.1 „Wzmocnienie bezpieczeństwa łańcucha dostaw na poziomie krajowym i międzynarodowym”, (ułatwienia zakupowe, pilotażowe wdrożenia i wsparcie certyfikacyjne dla rozwiązań krajowych producentów); wsparcie krajowych startupów

⁴ Tamże, cel szczegółowy 3, pkt 7.6 „Współpraca publiczno-prywatna w obszarze cyberbezpieczeństwa”

⁵ Tamże, cel szczegółowy 4, Zwiększanie potencjału krajowej bazy technologiczno-przemysłowej oraz wzmocnienie suwerenności technologicznej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.

i komponentów open source oraz usług podmiotów trzecich. Sam fakt takiego wykorzystania nie jest problemem; zasadniczą kwestią pozostaje brak wiedzy o tym, co dokładnie znajduje się „pod maską” ocenianego rozwiązania.

Coraz częściej dostawcy są w stanie dostarczyć zestawienie komponentów wykorzystanych w produkcie, znane jako spis materiałowy oprogramowania (ang. *Software Bill of Materials* - SBOM). Taki dokument pozwala zamawiającemu zrozumieć, z jakich elementów zbudowane jest rozwiązanie, jakie mają one pochodzenie i jurysdykcję, oraz czy wśród nich znajdują się komponenty, które w przeszłości były źródłem poważnych podatności bezpieczeństwa. Żądanie takiego zestawienia na etapie oceny oferty jest dobrą praktyką, która w naturalny sposób premiuje dostawców transparentnych i dojrzałych w zarządzaniu własnym łańcuchem dostaw, niezależnie od tego, czy jest to duża, globalna firma, czy mały, krajowy zespół.

Warto też pamiętać, że dostawca może być formalnie polski, a jednocześnie budować swój produkt niemal wyłącznie na komponentach pochodzących spoza Unii Europejskiej – i odwrotnie, produkt globalnego producenta może w praktyce opierać się na bardzo zróżnicowanym, dobrze udokumentowanym ekosystemie komponentów. **To kolejny argument za tym, żeby pytanie o przejrzystość łańcucha dostaw komponentów zadawać każdemu dostawcy w ten sam sposób, jako stały element oceny technicznej, a nie jako wyjątkowe wymaganie stosowane wybiórczo.**

Włączenie takiego pytania do standardowego procesu oceny nie musi oznaczać dodatkowego formalnego wymogu w dokumentacji postępowania – równie skutecznie można je zadać w ramach rozmowy technicznej lub testu praktycznego, opisanych we wcześniejszych rozdziałach tego poradnika. Chodzi przede wszystkim o to, żeby świadomość istnienia tego wymiaru oceny stała się naturalnym elementem pracy zespołu odpowiedzialnego za wybór rozwiązania, niezależnie od formy, w jakiej pytanie zostanie ostatecznie zadane.

10. Rola zamawiającego jako pierwszego klienta

Administracja publiczna i spółki Skarbu Państwa są w Polsce największym odbiorcą rozwiązań cyberbezpieczeństwa. To daje im rolę, która wykracza poza zwykłego kupującego – w praktyce to właśnie decyzje zakupowe sektora publicznego w dużej mierze decydują o tym, które innowacyjne produkty mają w ogóle szansę dojrzeć do skali, na której mogą konkurować także za granicą.

Warto świadomie przyjąć tę rolę pierwszego, wymagającego klienta, takiego, który nie tylko kupuje gotowy, sprawdzony produkt, ale jest też gotów uczestniczyć w jego dojrzewaniu poprzez pilotaże, testy referencyjne i wdrożenia w ograniczonej skali,

zanim podejmie decyzję o pełnym wdrożeniu. Dla wielu innowacyjnych, mniejszych dostawców to właśnie brak pierwszego, wiarygodnego wdrożenia referencyjnego – a nie brak jakości produktu – jest głównym powodem, dla którego nie są w stanie skutecznie konkurować w kolejnych postępowaniach. **Pierwsze wdrożenie, nawet ograniczone zakresem, ma wartość nieproporcjonalnie większą niż jego formalna skala, ponieważ otwiera drogę do kolejnych klientów zarówno w kraju, jak i za granicą.**

Dobłą praktyką jest też traktowanie testów referencyjnych i programów pilotażowych jako stałego, a nie wyjątkowego elementu polityki zakupowej organizacji – z jasno określonym budżetem, harmonogramem i kryteriami sukcesu, pozwalającymi ocenić, czy dane rozwiązanie zasługuje na szersze wdrożenie. Taki model pozwala organizacji testować innowacyjne rozwiązania przy ograniczonym ryzyku, a jednocześnie realnie wspiera rozwój krajowego rynku technologicznego i to nie poprzez preferencje formalne, ale poprzez stworzenie przestrzeni, w której dobry produkt ma w ogóle szansę zostać zauważony i sprawdzony.

Warto też dostrzec efekt, który wykracza poza pojedynczą transakcję. Wdrożenie referencyjne w dużej, wymagającej instytucji publicznej działa jak dźwignia: dostawca, który przeszedł taki proces, jest w znacznie lepszej pozycji, by ubiegać się o kolejne kontrakty, także za granicą, gdzie referencje z sektora publicznego innego kraju bywają traktowane jako istotny sygnał wiarygodności. W tym sensie decyzja pojedynczej instytucji o przyjęciu roli pierwszego, wymagającego klienta ma znaczenie, które wykracza poza jej własne potrzeby operacyjne.

11. Kryteria pozacenowe w ocenie ofert

Cena pozostaje ważnym, ale nie jedynym kryterium, którym warto posługiwać się przy wyborze rozwiązania cyberbezpieczeństwa. Świadome włączenie do oceny kryteriów jakościowych i innowacyjnych pozwala urealnić porównanie ofert, które na pierwszy rzut oka różnią się głównie kosztem, a w rzeczywistości oferują zupełnie inną wartość w dłuższym horyzoncie.

Do kryteriów jakościowych, które warto rozważyć obok ceny, należą między innymi: czas reakcji na zgłoszenie i lokalizacja zespołu wsparcia, dostępność środowiska testowego przed zakupem, elastyczność licencjonowania i możliwość dostosowania zakresu usługi do zmieniających się potrzeb organizacji, poziom dokumentacji technicznej oraz jakość i częstotliwość aktualizacji bezpieczeństwa. Żadne z tych kryteriów nie jest specyficzne dla dostawców polskich czy zagranicznych – są to

uniwersalne wymiary jakości, które po prostu rzadziej trafiają do specyfikacji niż parametry techniczne łatwe do skopiowania z materiałów producenta.

Warto też pamiętać, że kryteria jakościowe i innowacyjne mają największą wartość wtedy, gdy są mierzalne i możliwe do zweryfikowania, a nie sformułowane w sposób ogólnikowy, trudny do obiektywnej oceny. **Zamiast ogólnego postulatu „innowacyjności rozwiązania”, warto zdefiniować konkretne, sprawdzalne parametry takie jak: czas wykrycia i reakcji na określony typ zagrożenia, zakres automatyzacji procesu, poziom integracji z istniejącymi systemami organizacji.** Tak sformułowane kryteria dają się ocenić w sposób obiektywny, niezależnie od tego, kto składa ofertę, i jednocześnie realnie premiąją rozwiązania rzeczywiście nowocześniejsze, a nie tylko lepiej opisane marketingowo.

12. Jak organizować proces zakupowy, żeby ocena była możliwa

Nawet najlepiej zdefiniowane kryteria oceny nie przyniosą efektu, jeśli sam proces zakupowy nie daje przestrzeni na ich zastosowanie. Kilka praktycznych obserwacji prezentujemy poniżej, a które warto uwzględnić przy planowaniu postępowania.

Warto zaplanować czas i przestrzeń na **dialog techniczny** przed formalnym rozpoczęciem postępowania. **Rozmowa z kilkoma potencjalnymi dostawcami – w tym z mniejszymi, mniej rozpoznawalnymi firmami – zanim powstanie ostateczny opis przedmiotu zamówienia, pozwala zrozumieć pełne spektrum dostępnych na rynku rozwiązań, zamiast opisywać wymagania wyłącznie na podstawie znajomości jednego, dominującego produktu.** Tego rodzaju wstępne konsultacje rynkowe są dziś standardową praktyką, coraz częściej stosowaną świadomie przez najbardziej dojrzałe zakupowo instytucje.

Warto rozważyć włączenie do procesu etapu praktycznej weryfikacji rozwiązania – **testu w warunkach zbliżonych do docelowych** – szczególnie w przypadku zakupów o wyższej wartości lub istotnym znaczeniu dla bezpieczeństwa organizacji. Taki etap wymaga dodatkowego czasu i zasobów na etapie przygotowania postępowania, ale w praktyce znacząco redukuje ryzyko wyboru rozwiązania, które na papierze spełnia wszystkie wymagania, a w rzeczywistej pracy okazuje się niedopasowane.

Warto też, tam gdzie to możliwe, dzielić większe zamówienia na mniejsze, samodzielne części funkcjonalne, zamiast łączyć wiele różnych potrzeb technologicznych w jedno duże postępowanie. Duże, złożone zamówienia w naturalny sposób premiąją dostawców dysponujących szerokim portfolio gotowych, zintegrowanych rozwiązań, co często wyklucza możliwość udziału firm

wyspecjalizowanych w jednym, węższym obszarze, nawet jeśli w tym obszarze oferują rozwiązanie lepsze niż część szerszego pakietu konkurenta.

Wreszcie **warto budować w organizacji kompetencję do oceny technicznej niezależną od materiałów marketingowych i zewnętrznych rankingów**. Zespół, który potrafi samodzielnie ocenić architekturę rozwiązania, przeprowadzić test funkcjonalny i zadać dostawcy trafne pytania techniczne, jest znacznie mniej zależny od uproszczonych wskaźników zewnętrznych – niezależnie od tego, jak uznane i wygodne w użyciu te wskaźniki się wydają. To inwestycja, która zwraca się w każdym kolejnym postępowaniu, nie tylko w ocenie rozwiązań cyberbezpieczeństwa.

Wszystkie opisane wyżej elementy – dialog techniczny, test praktyczny, podział zamówienia na mniejsze części, budowa kompetencji wewnętrznej – wymagają czasu, którego często brakuje w harmonogramie postępowania planowanego pod presją terminów budżetowych. **Dobłą praktyką jest uwzględnianie tego czasu już na etapie planowania rocznego lub wieloletniego planu zakupowego organizacji, a nie dopiero w momencie, gdy potrzeba zakupu staje się pilna**. Postępowanie przygotowywane w pośpiechu niemal zawsze wraca do najprostszego, najbardziej znanego rozwiązania – nie dlatego, że jest ono obiektywnie najlepsze, ale dlatego, że nie było czasu na sprawdzenie alternatyw.

13. Najczęstsze błędy przy ocenie innowacyjnych rozwiązań

Poza trzema przekonaniem opisany w wcześniejszym rozdziale, w praktyce zakupowej powtarza się kilka innych, mniej oczywistych błędów, które warto znać, żeby ich unikać.

Pierwszym jest ocenianie rozwiązania wyłącznie na podstawie prezentacji sprzedażowej lub środowiska demonstracyjnego przygotowanego specjalnie na potrzeby prezentacji, zamiast w warunkach zbliżonych do rzeczywistej pracy organizacji. Środowisko demonstracyjne jest z definicji zoptymalizowane pod kątem pokazania produktu w najlepszym możliwym świetle: nie odzwierciedla typowych problemów integracyjnych, obciążenia czy nietypowych przypadków, z którymi rozwiązanie będzie się mierzyć w codziennej pracy.

Drugim jest ograniczenie oceny wyłącznie do ceny zakupu i licencji, z pominięciem kosztów wdrożenia, integracji, szkolenia zespołu oraz przyszłej migracji. Rozwiązanie tańsze w zakupie może okazać się droższe w całym cyklu życia, jeśli wymaga rozbudowanej, kosztownej integracji lub generuje istotne ryzyko zależności w przyszłości.

Trzecim jest przeprowadzanie oceny technicznej bez udziału zespołu odpowiedzialnego za bezpieczeństwo i utrzymanie systemów, wyłącznie na poziomie decyzji administracyjnej lub zakupowej. Osoby, które będą na co dzień pracować z danym rozwiązaniem, mają zwykle najlepszy wgląd w to, czy realnie odpowiada ono na potrzeby organizacji. Ich udział w procesie oceny, nie tylko w procesie wdrożenia, znacząco zwiększa trafność decyzji.

Czwartym jest poleganie na jednym, zewnętrznym źródle opinii – niezależnie od tego, czy jest nim komercyjny ranking, rekomendacja innej instytucji czy opinia pojedynczego eksperta – zamiast zestawienia kilku niezależnych źródeł informacji z bezpośrednią weryfikacją własną. Żadne pojedyncze źródło, jakkolwiek uznane, nie zastąpi własnej, kontekstowej oceny potrzeb organizacji.

Piątym, szczególnie kosztownym błędem jest traktowanie wyboru technologii jako decyzji jednorazowej, podejmowanej raz na kilka lat i niepodlegającej rewizji aż do kolejnego przetargu. Rynek rozwiązań cyberbezpieczeństwa zmienia się dziś na tyle szybko, że produkt uznany za najlepszy w momencie zakupu może po jakimś czasie istotnie ustąpić miejsca nowszym rozwiązaniom – zarówno pod względem funkcjonalności, jak i faktycznego poziomu bezpieczeństwa. **Dobłą praktyką jest okresowy przegląd rynku, niezależnie od tego, czy zbliża się moment odnowienia umowy, pozwalający organizacji na bieżąco orientować się, czy jej obecne rozwiązania wciąż pozostają konkurencyjne.**

14. Jak czytać deklaracje i materiały marketingowe dostawców

Każdy dostawca, niezależnie od wielkości i pochodzenia, opisuje swój produkt w sposób możliwie korzystny – to naturalny element komunikacji rynkowej, a nie powód do nieufności. Warto jednak umieć odróżnić język, który da się zweryfikować, od języka, który brzmi przekonująco, ale niewiele mówi o rzeczywistych właściwościach rozwiązania.

Sformułowania takie jak „lider rynku”, „wykorzystujemy najnowocześniejszą sztuczną inteligencję” czy „zaufało nam setki klientów” są trudne do zweryfikowania bez dodatkowych, konkretnych danych i warto traktować je jako punkt wyjścia do pytania o szczegóły, a nie jako samodzielny dowód jakości. Znacznie bardziej wiarygodne są sformułowania odnoszące się do konkretnych, sprawdzalnych faktów: **nazwy konkretnych certyfikatów wraz z datą ich uzyskania, opis architektury technicznej możliwy do zweryfikowania podczas rozmowy z inżynierami, konkretne liczby dotyczące wydajności możliwe do sprawdzenia w teście.**

Dobłą praktyką jest teŹ zwracanie uwagi na to, czego materiały dostawcy nie mówią, a nie tylko na to, co mówią. Brak informacji o lokalizacji zespołu rozwojowego, o modelu przechowywania danych czy o polityce aktualizacji bezpieczeństwa jest sama w sobie informacją – wskazuje obszary, o które warto zapytać wprost, zanim zostaną one uznane za nieistotne.

Ten sam standard weryfikacji warto stosować symetrycznie, wobec materiałów każdego dostawcy, niezależnie od tego, czy jest to duża, rozpoznawana marka, czy mały, mniej znany podmiot. W obu przypadkach materiał marketingowy jest punktem wyjścia do rozmowy, a nie jej zakończeniem.

15. Zależność od dostawcy jako ryzyko do zarządzania

Każdy wybór technologiczny tworzy pewien poziom zależności od dostawcy – to naturalny element funkcjonowania każdej organizacji i nie da się go całkowicie wyeliminować. Różnica między zależnością zarządzaną a zależnością niekontrolowaną leŹy w tym, czy organizacja świadomie monitoruje jej poziom i konsekwencje, czy traktuje ją jako coś oczywistego, o czym nie trzeba myśleć, dopóki nie stanie się problemem.

Warto przy tym odróżnić zależność techniczną od zależności organizacyjnej.

Zależność techniczna dotyczy architektury systemu i możliwości jego zastąpienia innym rozwiązaniem. Zależność organizacyjna dotyczy tego, na ile procesy, procedury i nawyki pracy zespołu zostały zbudowane wokół konkretnego narzędzia w sposób, który sam w sobie utrudnia zmianę. Ten drugi rodzaj zależności bywa w praktyce trudniejszy do przezwyciężenia, bo rzadko jest w ogóle rozpoznawany jako zależność - funkcjonuje raczej jako „tak po prostu u nas działa”.

Dobłą praktyką jest okresowy przegląd portfela technologicznego organizacji pod kątem koncentracji zależności – czy kluczowe funkcje bezpieczeństwa opierają się na jednym dostawcy lub jednym ekosystemie technologicznym i jakie byłyby realne konsekwencje utraty dostępu do niego, niezależnie od przyczyny: upadłość firmy, zmiana polityki licencyjnej, decyzje regulacyjne w innej jurysdykcji czy zwykła eskalacja kosztów. Taki przegląd nie musi prowadzić do natychmiastowej zmiany dostawców. Jego celem jest świadomość, która pozwala podejmować lepsze decyzje w przyszłości, zamiast działać reaktywnie w sytuacji kryzysowej.

Dobłą praktyką jest teŹ, tam gdzie to uzasadnione ryzykiem, świadome utrzymywanie zdolności do wyboru m.in. poprzez budowanie architektury opartej na otwartych standardach, unikanie integracji, które nieodwracalnie wiążą organizację z jednym ekosystemem, oraz stosowanie mechanizmów kontraktowych, takich jak

zobowiązanie do deponowania kodu źródłowego, w przypadku współpracy z mniejszymi dostawcami. **Warto pamiętać, że tego rodzaju ryzyko dotyczy w równym stopniu dostawców dużych i małych – duży, globalny dostawca może równie skutecznie zmienić warunki licencyjne w sytuacji braku realnej alternatywy po stronie klienta, jak mały dostawca może zniknąć z rynku.**

Wreszcie, zachowanie realnej, wiarygodnej alternatywy technologicznej nawet jeśli aktualnie z niej nie korzystamy ma wartość samą w sobie. **Organizacja, która wie, że istnieje sprawdzona alternatywa dla używanego rozwiązania, negocjuje kolejne umowy z zupełnie innej pozycji niż organizacja, dla której zmiana dostawcy jest praktycznie niewyobrażalna.** Ta wiedza jest częścią realnej suwerenności technologicznej – nie w sensie deklaratywnym, ale w sensie praktycznej zdolności do podejmowania niezależnych decyzji.

Struktura własnościowa i ryzyko przejęcia

Osobnym, rzadziej rozważanym wymiarem zależności jest ryzyko związane ze zmianą struktury właścicielskiej dostawcy w przyszłości. Perspektywiczny, dobrze rozwijający się dostawca technologii bezpieczeństwa jest naturalnym celem przejęcia zarówno przez inwestorów finansowych, jak i przez większych, globalnych konkurentów. Przejęcie samo w sobie nie musi być problemem, ale warto mieć świadomość, że może prowadzić do zmiany priorytetów rozwoju produktu, zmiany polityki cenowej, a czasem do wygaszenia rozwiązania na rzecz produktu konkurencyjnego z portfela nowego właściciela.

Dobłą praktyką jest uwzględnianie tego ryzyka w ocenie długoterminowej stabilności dostawcy – niezależnie od tego, czy jest on dziś spółką polską, europejską czy globalną – oraz zabezpieczanie się poprzez mechanizmy kontraktowe, takie jak gwarancje kontynuacji wsparcia w przypadku zmiany właściciela, czy wspomniane wcześniej deponowanie kodu źródłowego. Warto też pamiętać, że ryzyko to działa w obie strony: równie dobrze może dotyczyć małego, polskiego startupu przejmowanego przez zagranicznego inwestora, jak i regionalnego oddziału dużego, globalnego producenta, którego priorytety mogą się zmienić niezależnie od potrzeb pojedynczego klienta w Polsce.

16. Jak zacząć

Wdrożenie opisanych w tym poradniku praktyk nie musi i nie powinno zaczynać się od razu we wszystkich obszarach działania organizacji. Naturalnym punktem wyjścia

jest wybór jednego, najbliższego terminowo postępowania o umiarkowanej skali, w którym można świadomie zastosować kilka z opisanych tu zasad.

1. Sformułować opis przedmiotu zamówienia wokół efektu i mierzalnych parametrów, a nie wokół konkretnej marki lub technologii.
2. Przeprowadzić krótki dialog techniczny z kilkoma potencjalnymi dostawcami, zanim powstanie ostateczna wersja specyfikacji.
3. Włączyć do oceny prosty test praktyczny (proof of concept) zamiast polegania wyłącznie na dokumentach i referencjach.

Doświadczenie zdobyte przy takim pierwszym, ograniczonym postępowaniu – zarówno to, co się udało, jak i to, co okazało się trudniejsze niż zakładano – jest znacznie cenniejsze niż próba jednoczesnej zmiany całej polityki zakupowej organizacji. Kolejne postępowania mogą stopniowo obejmować więcej z opisanych tu praktyk, w miarę jak zespół zdobywa pewność i wypracowuje własne, dopasowane do specyfiki organizacji sposoby ich stosowania.

17. Podsumowanie

Ocena innowacyjności i suwerenności technologicznej produktu cyberbezpieczeństwa nie wymaga rewolucji w procesie zakupowym – wymaga raczej świadomego przesunięcia punktu ciężkości: od pytania, czy dany dostawca jest wystarczająco duży i rozpoznawalny, do pytania, czy jego rozwiązanie rzeczywiście robi to, czego potrzebuje organizacja, i czy zachowuje ona nad nim realną kontrolę.

Praktyki opisane w tym poradniku – ocena efektu zamiast marki, bezpośrednia weryfikacja techniczna zamiast polegania wyłącznie na referencjach i rankingach, rozdzielenie oceny skalowalności produktu od wielkości firmy dostawcy, świadome liczenie kosztu zależności w długim horyzoncie oraz konsekwentne zadawanie pytań o własność intelektualną, lokalizację rozwoju, jurysdykcję i zdolność do migracji – nie są zarezerwowane dla oceny polskich dostawców. Są to praktyki, które warto stosować wobec każdej oferty, niezależnie od jej pochodzenia. To właśnie ich konsekwentne, niewybiórcze stosowanie odróżnia rzetelną, profesjonalną politykę zakupową od przypadkowości – i to ono, jako efekt uboczny, otwiera realną przestrzeń dla rozwiązań, które dziś przegrywają nie dlatego, że są gorsze, ale dlatego, że nie miały szansy zostać ocenione na równych zasadach.

Zbudowanie takiej praktyki w organizacji to proces, nie jednorazowa decyzja. Każde kolejne postępowanie, w którym opis przedmiotu zamówienia koncentruje się na efekcie i mierzalnych parametrach, w którym znajduje się miejsce na test praktyczny,

w którym pytania o własność intelektualną i zdolność do migracji są zadawane rutynowo, to krok w stronę organizacji, która świadomie zarządza swoją zależnością technologiczną, zamiast być przez nią zaskakiwana.

Dla całego ekosystemu cyberbezpieczeństwa w Polsce efekt takiej zmiany, powtórzonej w skali wielu organizacji publicznych, byłby więcej niż sumą pojedynczych, lepszych decyzji zakupowych. To właśnie decyzje zamawiających – konsekwentnie stosowane, oparte na jasnych, uniwersalnych kryteriach – tworzą warunki, w których jakość i innowacyjność mogą rzeczywiście decydować o wyborze technologii.

18. Słownik pojęć

- Suwerenność technologiczna – Zdolność organizacji do świadomego kontrolowania, rozwijania i bezpiecznego utrzymywania kluczowych systemów cyfrowych, przy zachowaniu realnej możliwości zmiany dostawcy bez paraliżu operacyjnego.
- Zależność od dostawcy (*ang. vendor lock-in*) – Sytuacja, w której koszt lub złożoność zmiany dostawcy technologii staje się na tyle wysoka, że organizacja traci realną zdolność wyboru, mimo formalnego prawa do zmiany.
- Dowód koncepcji (*ang. Proof of concept - PoC*) – Praktyczny test rozwiązania w warunkach zbliżonych do docelowych, przeprowadzany przed podjęciem ostatecznej decyzji zakupowej.
- Deponowanie kodu źródłowego (*ang. software escrow*) – Mechanizm polegający na zdeponowaniu kodu źródłowego produktu u zaufanej trzeciej strony, udostępnianego klientowi w określonych, z góry ustalonych okolicznościach, np. w przypadku zaprzestania działalności przez dostawcę.
- Interoperacyjność – Zdolność systemu do współdziałania z innymi rozwiązaniami, zwykle dzięki oparciu na otwartych standardach i udokumentowanych interfejsach.
- Całkowity koszt posiadania (*ang. Total Cost of Ownership - TCO*) – Całkowity koszt posiadania rozwiązania w danym horyzoncie czasowym, uwzględniający nie tylko koszt zakupu i utrzymania, ale też potencjalny koszt migracji do innego rozwiązania w przyszłości.
- Dialog techniczny / konsultacje rynkowe – Wstępna, poprzedzająca formalne postępowanie rozmowa z potencjalnymi dostawcami, pozwalająca lepiej rozpoznać dostępne na rynku rozwiązania przed sformułowaniem ostatecznych wymagań.
- Pierwszy klient / anchor tenant – Organizacja, zwykle o dużej skali działania, która jako jedna z pierwszych decyduje się na wdrożenie nowego, niesprawdzonego jeszcze na szeroką skalę rozwiązania, umożliwiając jego dalszy rozwój i budowę wiarygodności rynkowej.
- Wyjaśnialność modelu (*ang. explainability*) – Zdolność systemu opartego na sztucznej inteligencji do przedstawienia zrozumiałego dla człowieka uzasadnienia podjętej decyzji lub rekomendacji, a nie wyłącznie samego wyniku.
- Otwarte standardy – Publicznie dostępne, niezależne od jednego producenta specyfikacje techniczne, których stosowanie ułatwia integrację i migrację między różnymi systemami.

19. O klastrze CyberMadeInPoland

Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland zrzesza polskie firmy, instytucje naukowe i organizacje działające w obszarze cyberbezpieczeństwa. Celem klastra jest budowanie konkurencyjności krajowego sektora, wspieranie ekspansji zagranicznej polskich firm technologicznych oraz dialog między biznesem, nauką i administracją publiczną na rzecz dojrzałego, odpornego ekosystemu cyberbezpieczeństwa w Polsce.

Poradnik powstał w ramach udziału w programie PWCyber.

Więcej informacji: [CyberMadeInPoland](#)