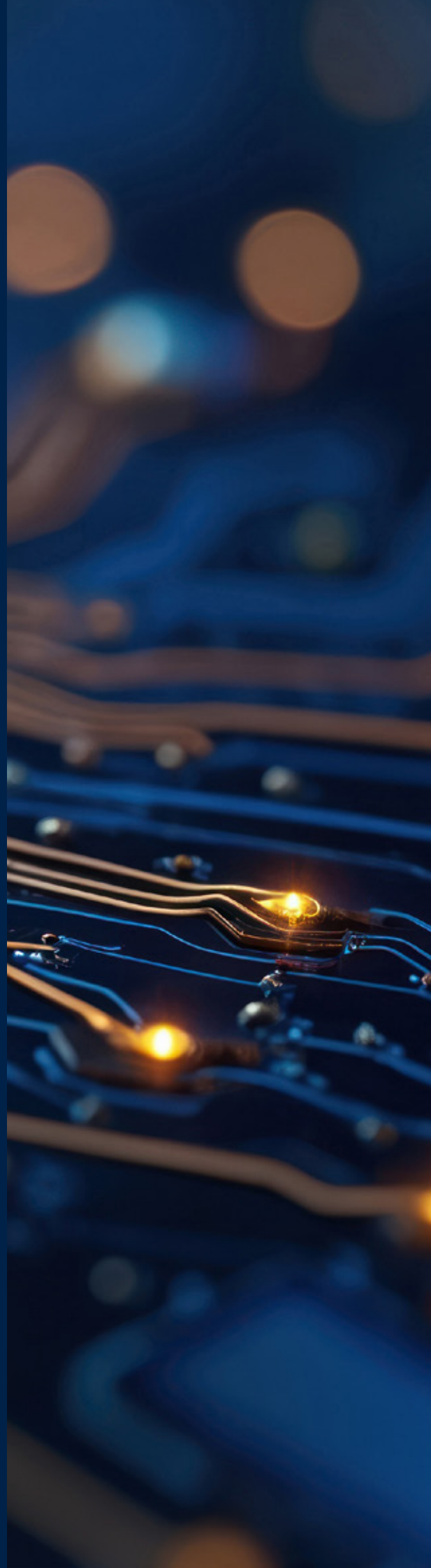


Jak zapewnić
ciągłość działania?
*Przewodnik
po suwerenności
cyfrowej*

BEST PRACTICE GUIDE

Zapewnienie ciągłości działania: przewodnik po suwerenności cyfrowej	03
Siedem filarów budowania cyfrowej niezależności w firmie:	04
1. Alternatywy open source	04
2. Technologia wyprodukowana w UE	05
3. Dane w chmurze	06
4. On-premises zamiast chmury	07
5. Pociąganie partnerów do odpowiedzialności	08
6. Opracuj strategię wyjścia	09
7. Co-management i dywersyfikacja	10
Wnioski i perspektywy	11
Kontakt	13



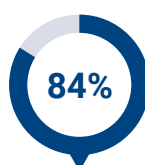
Zapewnienie ciągłości działania: przewodnik po suwerenności cyfrowej

W coraz bardziej połączonym i opartym na danych świecie suwerenność cyfrowa przestała być jedynie modnym hasłem – stała się kluczowym czynnikiem sukcesu przedsiębiorstw. Ścisła integracja z partnerami biznesowymi, korzystanie z usług w chmurze i modele biznesowe oparte na danych stwarzają ogromne możliwości. Wymagają one jednak krytycznej oceny.



Uzależnienie od zagranicy

96% przedsiębiorstw w UE korzysta z technologii cyfrowych i usług spoza Europy – zwłaszcza ze Stanów Zjednoczonych i Chin



Zwolennicy

84,4% decydentów IT preferuje wykorzystanie europejskich produktów cyfrowych w obszarze infrastruktury krytycznej, ale tylko 20% organizacji znajduje się obecnie w procesie ich wdrażania



Cel strategiczny

87% firm postrzega niezależność cyfrową jako cel strategiczny, ale 79% jest krytycznie uzależnionych od kilku, głównie pozaeuropejskich dostawców mostly

Według badania przeprowadzonego przez adesso i Instytut Badawczy Handelsblatt, brak kompetencji, niedobór wykwalifikowanych pracowników i wysokie koszty wciąż hamują rozwój suwerenności cyfrowej w wielu organizacjach.

Suwerenność cyfrowa nabiera coraz większego znaczenia, szczególnie w obliczu globalnej niepewności, rosnących zagrożeń cybernetycznych i coraz bardziej złożonych wymogów regulacyjnych. Zachowanie kontroli nad własnymi danymi, infrastrukturą i procesami cyfrowymi ma kluczowe znaczenie dla uniknięcia zależności od zewnętrznych dostawców, platform czy interesów geopolitycznych. Celem jest zapewnienie ciągłości działania, minimalizacja ryzyka i utrzymanie długoterminowej konkurencyjności.



Siedem filarów budowania cyfrowej niezależności w firmie:

1. Alternatywy open source

Znaczna część oprogramowania używanego na co dzień w pracy biurowej pochodzi od dużych korporacji, które nierzadko stosują jednostronne lub restrykcyjne modele licencyjne. Firmy uzależnione wyłącznie od zamkniętych ekosystemów (ang. walled gardens) mogą bardzo łatwo znaleźć się pod presją takich dostawców. Alternatywą jest korzystanie z bezpłatnego oprogramowania open source, które zapewnia m.in.:

- ✓ **Oszczędność kosztów licencyjnych**
- ✓ **Uniknięcie zależności od poszczególnych producentów**
- ✓ **Często wyższy poziom bezpieczeństwa dzięki systematycznej weryfikacji kodu źródłowego i lepszej możliwości audytu**
- ✓ **Szerokie wsparcie społeczności użytkowników oraz deweloperów**

PRZYKŁADÓW SPRAWDZONYCH

Do znanych przykładów sprawdzonych, profesjonalnych rozwiązań open source należą LibreOffice, edytor graficzny GIMP, system operacyjny Linux, przeglądarka Mozilla Firefox oraz klient poczty Thunderbird.

2. Technologia wyprodukowana w UE

Suwerenność danych zależy od jurysdykcji, której podlega partner technologiczny. Jeśli rząd danego kraju zmusi partnera do ujawnienia danych, nawet najstaranniej skonstruowane umowy nie zagwarantują ich pełnej ochrony. Jedynym rozwiązaniem jest staranny dobór dostawcy. UE i państwa z nią stowarzyszone posiadają jedno z najbardziej surowych regulacji dotyczących:

- **Ochrony danych**
(RODO, TISAX, DORA)
- **Ochrony konsumentów**
(Akt o Sprawiedliwości Cyfrowej,
Akt o Usługach Cyfrowych)
- **Obowiązków należytej staranności**
(Akt ws. danych (Data Act),
ustawa UE o łańcuchu dostaw)

Oprogramowanie i usługi z krajów UE stanowią zatem solidną inwestycję z punktu widzenia ochrony danych i infrastruktury – gwarantują pewność prawną i możliwość skutecznego egzekwowania praw na drodze sądowej. Ma to szczególne znaczenie przy wyborze dostawcy usług w chmurze. Nawet jeśli serwery centrum danych fizycznie znajdują się w UE, kluczowe znaczenie ma kraj, **w którym zarejestrowana jest siedziba firmy.**



3. Dane w chmurze

Przechowywanie danych w chmurze nie powinno bazować wyłącznie na zabezpieczeniach oferowanych przez dostawcę. Nawet organizacje korzystające wyłącznie z usług chmurowych, których centra danych zlokalizowane są w UE, gdzie obowiązują rygorystyczne przepisy o ochronie danych, powinny zadbać o następujące kwestie:

Szyfrowanie:

skuteczna ochrona danych wymaga, aby nawet dostawca chmury nie miał dostępu do danych w postaci niezaszyfrowanej. Organizacje stosujące szyfrowanie wykazują się odpowiedzialnością i budują zaufanie do swoich procesów cyfrowych.

Koncepcje usuwania danych:

po wygaśnięciu umowy należy upewnić się, że dane zostały rzeczywiście i trwale usunięte.

Koncepcje autoryzacji:

korzystanie z usług w chmurze wymaga przemyślanych i niezawodnych modeli autoryzacji oraz zarządzania uprawnieniami dostępu. Obowiązuje tu zasada „tak dużo, ile konieczne – tak mało, jak to możliwe”.



Wdrożenie tych środków pozwala osiągnąć wysoki stopień bezpieczeństwa i niezależności.



4. On-premises zamiast chmury

Usługi w chmurze są wyjątkowo atrakcyjne ze względu na wygodę i skalowalność. Jednak ich wykorzystanie oznacza powierzenie własnych danych podmiotom zewnętrznym. **Jeśli chcesz tego uniknąć, warto rozważyć powrót do rozwiązań lokalnych (on-premises), które oferują następujące korzyści:**

- ✓ **Brak dostępu osób trzecich do wrażliwych zasobów cyfrowych**
- ✓ **Często lepsza opłacalność w dłuższej perspektywie**
- ✓ **Szybsze rozwiązywanie problemów przez własnych pracowników**



Aby jednak rozwiązania lokalne przyniosły oczekiwane rezultaty, firmy muszą z wyprzedzeniem inwestować w odpowiednie kompetencje i infrastrukturę techniczną wewnątrz organizacji.

5. Pociąganie partnerów do odpowiedzialności

Suwerenność cyfrowa jest możliwa do osiągnięcia tylko wtedy, gdy organizacje dbają nie tylko o bezpieczeństwo własnych systemów i procesów, lecz także konsekwentnie egzekwują określone standardy również od swoich partnerów. Podmioty technologiczne i usługowe działające na różnych etapach łańcucha dostaw mają bezpośredni wpływ na przetwarzanie wrażliwych danych i utrzymanie infrastruktury cyfrowej. Dlatego niezbędne jest ustanowienie jasnych regulacji umownych dotyczących przetwarzania i przechowywania danych oraz standardów bezpieczeństwa.



Przejrzystość

Wymagaj od partnerów pełnej przejrzystości w tym zakresie.



Ujawnienie

Nalegaj na pełną transparentność podwykonawców i ich lokalizacji, by jak najwcześniej zidentyfikować i ocenić potencjalne ryzyka wynikające z dostępu do naszych danych zagranicznych organów prawnych, np. na podstawie przepisów CLOUD Act lub analogicznych regulacji.



Zabezpieczenie

Zadbaj, aby umowy jednoznacznie regulowały ochronę przed nieautoryzowanym dostępem osób trzecich i określały wiążące mechanizmy bezpieczeństwa informacji, takie jak szyfrowanie i kontrola dostępu.



Certyfikaty

Zapisz w umowie obowiązek regularnych audytów i certyfikacji (np. ISO 27001), aby móc weryfikować zgodność z deklarowanymi standardami.



6. Opracuj strategię wyjścia

Z czasem może się okazać, że dotychczasowi partnerzy technologiczni lub usługowi przestają spełniać wymagania dotyczące bezpiecznego i zgodnego z prawem przetwarzania danych. Przyczyn może być wiele: zmiana modeli biznesowych, incydenty bezpieczeństwa, brak przejrzystości, a nawet nowe uwarunkowania geopolityczne. Aby zachować ciągłość działania w takich sytuacjach, warto z wyprzedzeniem zidentyfikować alternatywy dla wszystkich systemów i usług o krytycznym znaczeniu oraz opracować konkretne strategie zakończenia współpracy.

Taka strategia powinna precyzyjnie definiować procesy oraz jasno przypisywać odpowiedzialności, tak aby ewentualna zmiana rozwiązania przebiegła w sposób uporządkowany i z minimalnymi zakłóceniami dla organizacji.



Zadanie 1

Przeprowadzaj regularne inwentaryzacje, aby sprawdzić, jakie usługi są wykorzystywane w poszczególnych obszarach firmy i jakie alternatywy są dostępne.

Zadanie 2

Opracuj proces określający zarówno procedury zmiany usługi lub technologii, jak i podział odpowiedzialności.

Zadanie 3

Określ terminy usunięcia danych przez poprzedniego partnera i zażądaj pisemnego potwierdzenia ich całkowitego usunięcia.

7. Co-management i dywersyfikacja

Suwerenność cyfrowa to niezależność od konkretnych rozwiązań technologicznych. Dlatego firmy nie powinny uzależniać się od jednego dostawcy, lecz stawiać na dywersyfikację.

Jednoczesne korzystanie z kilku kompatybilnych systemów zwiększa niezawodność i pozwala na utrzymanie ciągłości działania w przypadku awarii lub ograniczeń dostępności jednego z rozwiązań.

Współzarządzanie wspiera to podejście poprzez:

- **Jednoczesne zarządzanie na różnych platformach**
- **elastyczność infrastruktury IT zgodnie z koncepcją „best of breed”**
- **unikanie efektu uzależnienia od dostawcy (ang. vendor lock-in)**

Łącząc dywersyfikację ze współzarządzaniem, firmy zachowują kontrolę nad swoimi procesami cyfrowymi i są w stanie szybciej reagować na zmiany – niezależnie od tego, czy mają one podłoże techniczne, ekonomiczne czy regulacyjne.



Wnioski i perspektywy

Suwerenność cyfrowa to nie jednorazowy projekt, lecz ciągły proces wymagający strategicznego myślenia, wiedzy technologicznej i przejrzystości organizacyjnej. Firmy, które już dziś obiorą właściwy kierunek, zapewnią sobie niezależność i elastyczność niezbędną w przyszłości do skutecznego reagowania na zmieniające się warunki.



Przeanalizuj istniejące zależności cyfrowe, wyznacz jasne cele w zakresie większej autonomii cyfrowej i konsekwentnie je realizuj.



Teraz jest odpowiedni moment,
aby podjąć działania.

O firmie baramundi software GmbH

baramundi software to dostawca zunifikowanego oprogramowania do zarządzania punktami końcowymi, przeznaczonego do centralnego zarządzania komputerami PC, urządzeniami mobilnymi i serwerami. Automatyzuje ono dystrybucję oprogramowania, upraszcza zarządzanie poprawkami i zapewnia przejrzystość sieci. W ten sposób baramundi istotnie przyczynia się do poprawy bezpieczeństwa cyfrowego i uwalnia czas administratorów IT.



Masz pytania?

Zapraszamy do umówienia się na spotkanie.

Podczas spotkania wyjaśnimy, w jaki sposób oprogramowanie baramundi może pomóc Ci osiągnąć większą niezależność cyfrową dzięki zunifikowanemu rozwiązaniu do zarządzania punktami końcowymi.



Napisz do nas.
Czekamy na Ciebie!



Making IT Admins Smile



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany
+49 821 56708-380
request@baramundi.com



+43 1 928 0136 0010
request@baramundi.com



+41 77 280 49 79
request@baramundi.com



+39 340 8861886
request-italia@baramundi.com



+48 735 91 44 54
request@baramundi.com



+44 2071 93 28 77
request@baramundi.com



baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA
+1 508 861 7561
requestUSA@baramundi.com



+49 821 56708-390
request@baramundi.com