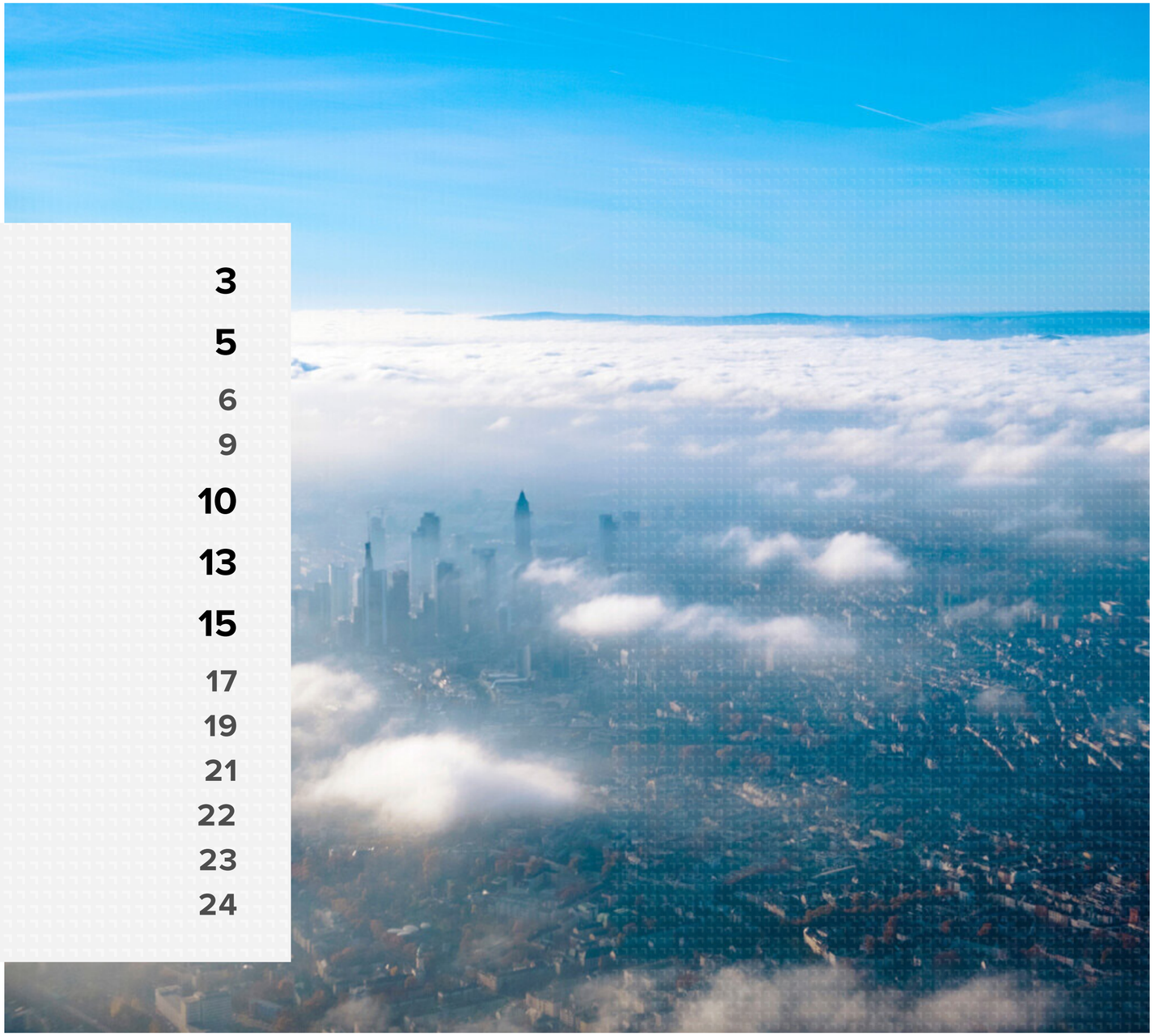
GFT

Hardening usługi | Sierpień 2023

Azure Container Apps

Agenda

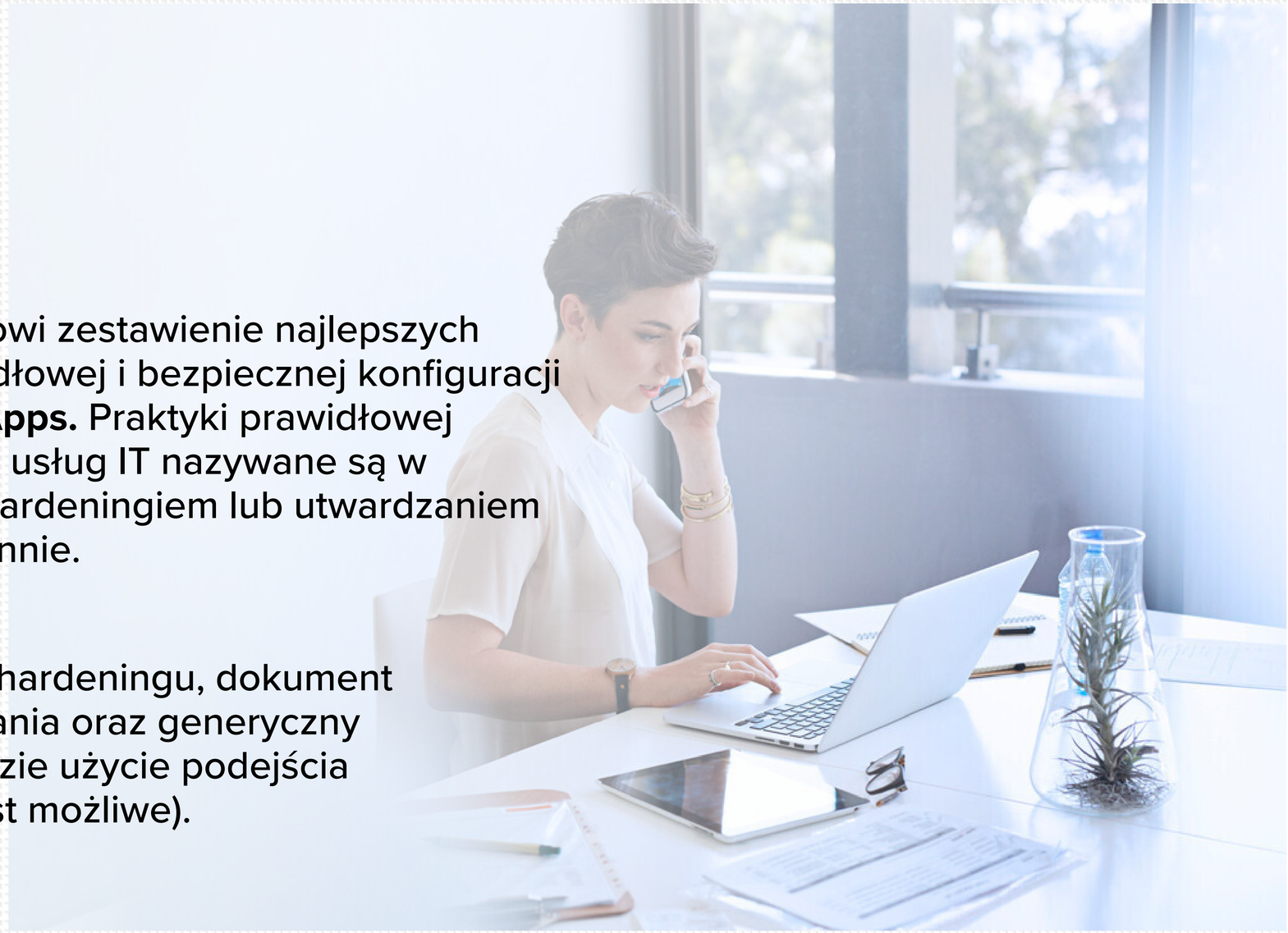


01 Wprowadzenie

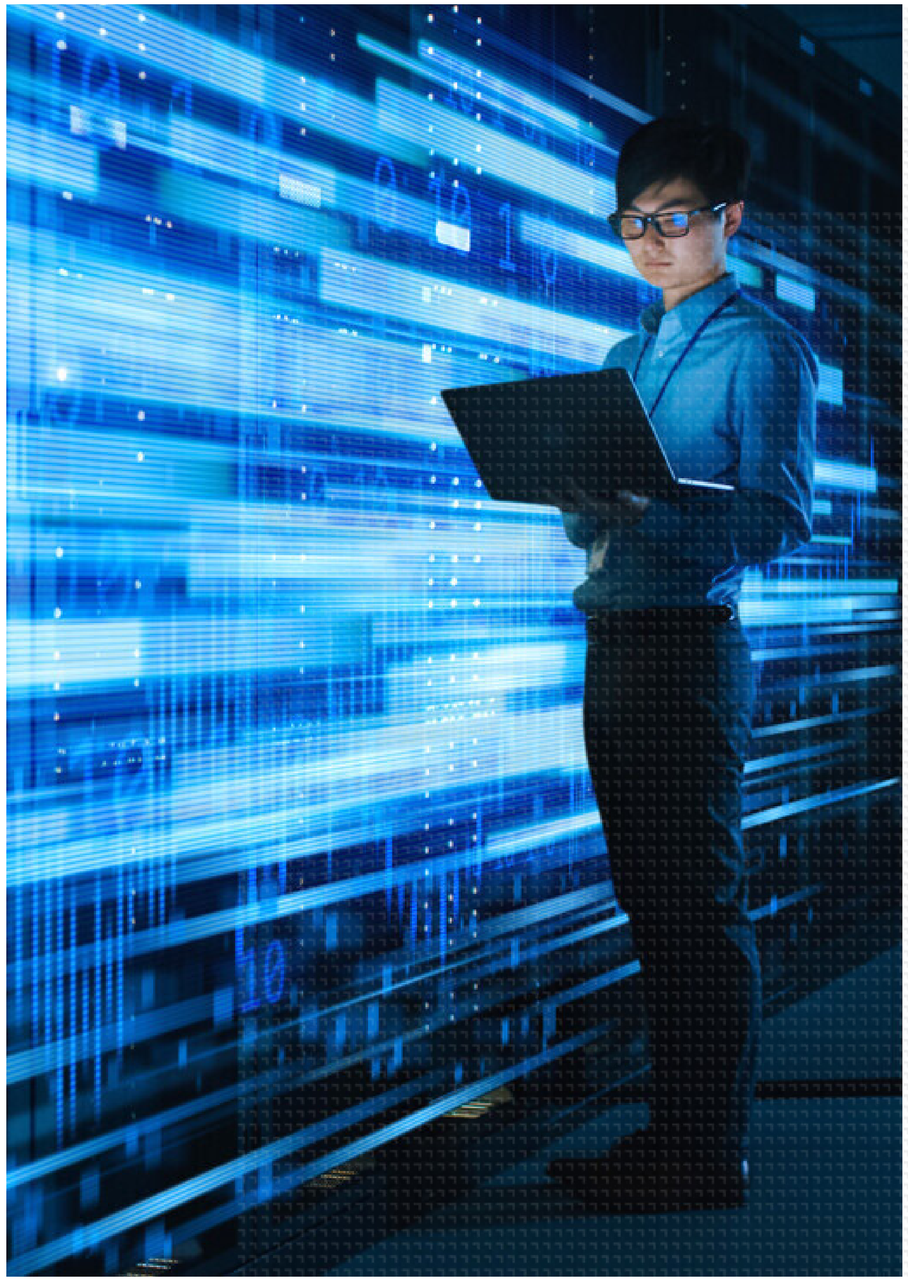
1 Wprowadzenie

Niniejszy dokument stanowi zestawienie najlepszych praktyk w zakresie prawidłowej i bezpiecznej konfiguracji usługi **Azure Container Apps.** Praktyki prawidłowej i bezpiecznej konfiguracji usług IT nazywane są w niniejszym dokumencie hardeningiem lub utwardzaniem oraz są stosowane zamiennie.

Dla każdego wymagania hardeningu, dokument przedstawia opis wymagania oraz generyczny skrypt Terraform (tam, gdzie użycie podejścia Infrastructure as Code jest możliwe).



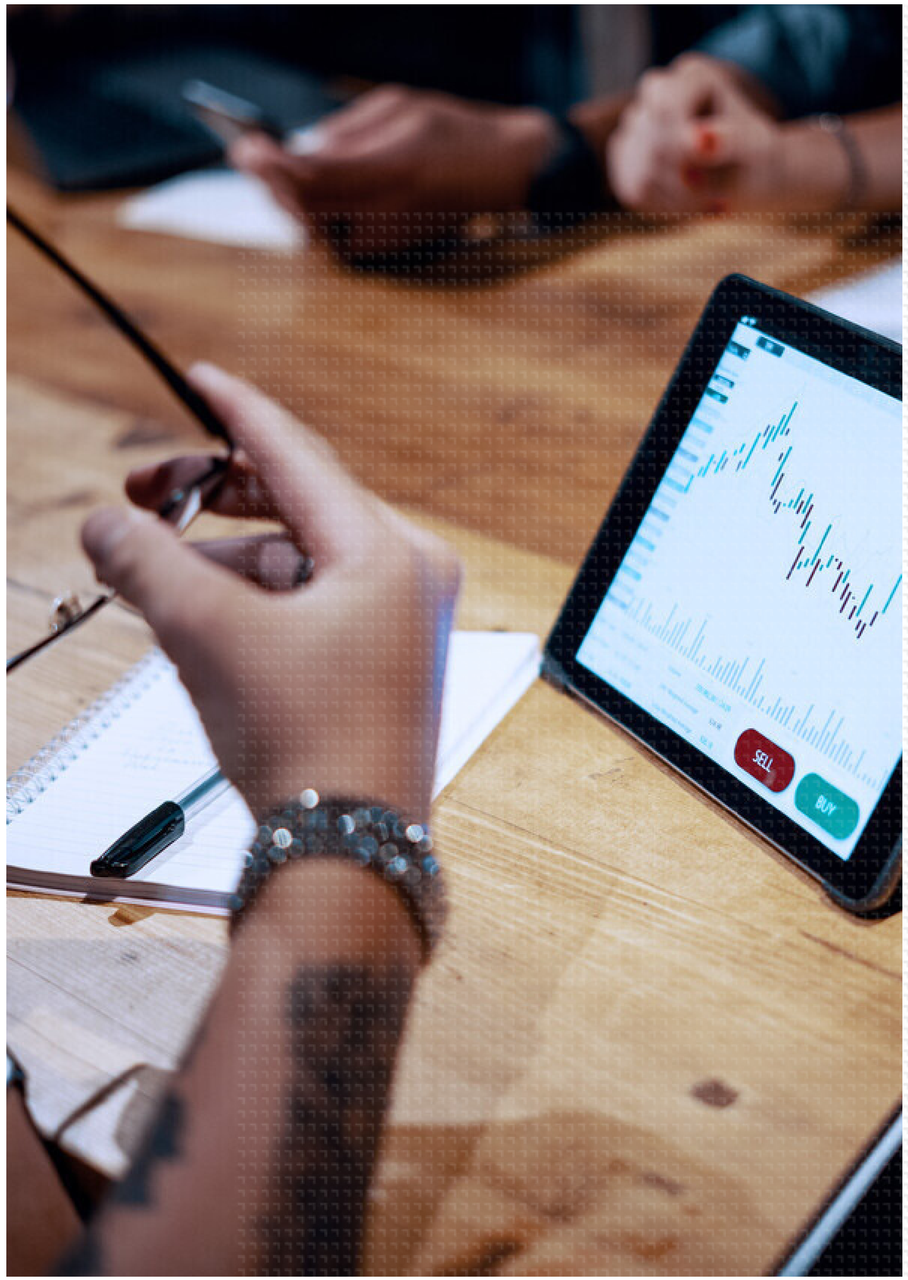
02
Usługa Azure Container Apps



2.1 Podstawowe informacje

Azure Container Apps to usługa serwerowa do budowania i wdrażania nowoczesnych aplikacji i mikrousług przy użyciu kontenerów. Typowe zastosowania Azure Container Apps to:

- wdrażanie punktów końcowych API
- obsługa przetwarzania w tle
- przetwarzanie zdarzeń
- uruchamianie mikrousług



2.1 Podstawowe informacje c.d.

Usługa Azure Container Apps jest przydatna dla Platform Engineering oraz Internal Developer Platforms, ponieważ:

- umożliwia wdrażanie aplikacji skonteneryzowanych bez zarządzania złożoną infrastrukturą,
- umożliwia uruchamianie kontenerów oraz ich skalowanie w odpowiedzi na ruch HTTP lub rosnącą liczbę wyzwalaczy skalowania obsługiwanych przez Kubernetes Event-Driven Autoscaling (KEDA) - takich jak Azure Event Hub, Apache Kafka, RabbitMQ Queue, MongoDB, MySQL i PostgreSQL,
- umożliwia pisanie kodu w preferowanym języku i przyspiesza rozwój aplikacji dzięki wbudowanej integracji z Distributed Application Runtime (Dapr), która upraszcza typowe zadania takie jak przetwarzanie zdarzeń, pub/sub i wywoływanie usług.

2.1 Podstawowe informacje c.d.

- Środowisko chmurowe Microsoft Azure daje możliwość **zbudowania skonteneryzowanych aplikacji** w oparciu o kilka rozwiązań. Główne zastosowanie usługi Azure Container Apps to budowa aplikacji w oparciu o **Kubernetes bez bezpośredniego dostępu do wszystkich natywnych interfejsów API Kubernetes oraz zarządzania klastrami.**

- W przypadku, gdy wymagany jest dostęp do interfejsów API Kubernetes i płaszczyzny sterowania, należy użyć usługi **Azure Kubernetes Service,** zaś w przypadku budowania aplikacji webowych najlepszą opcją będzie **Azure App Service.**

2.2 Ograniczenia usługi

Usługa posiada ograniczenia, które zostały przedstawione w poniższej tabeli.

REF	Nazwa ograniczenia	Opis ograniczenia oraz jego wpływ na usługę
2.2.01	Ograniczenie w obrazach kontenerów	Usługa Azure Container Apps umożliwia korzystanie jedynie z obrazów kontenerów bazujących na systemie Linux (linux/amd64). https://learn.microsoft.com/en-us/azure/container-apps/containers#limitations
		po więcej szczegółów skontaktuj się z naszym konsultantem

03
Rodzaje wymagań hardeningu

3 Rodzaje wymagań hardeningu

Rodzaje wymagań hardeningu przedstawionych w niniejszym dokumencie:

specyficzne dla usługi

występują tylko dla omawianej usługi i wynikają z rekomendacji Microsoftu oraz najlepszych praktyk GFT Poland,

specyficzne dla Microsoft Azure

dotyczą szeregu usług Azure w podobnym lub jednakowym zakresie dla omawianej usługi i wynikają z rekomendacji Microsoftu oraz najlepszych praktyk GFT Poland,

generalne

stanowią implementację najlepszych praktyk GFT Poland w zakresie bezpieczeństwa informacji w systemach informatycznych.

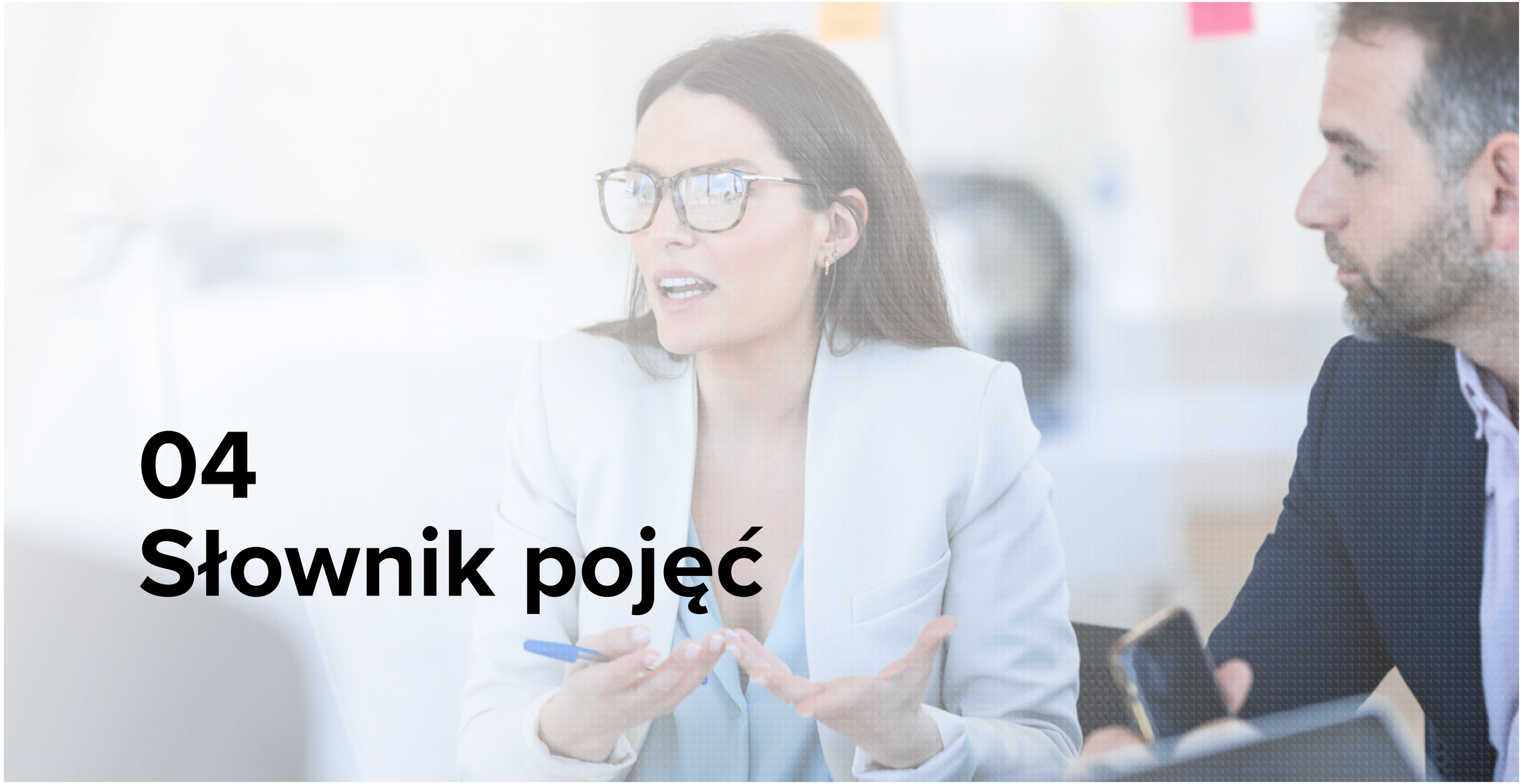
3 Rodzaje wymagań hardeningu

Wymagania mogą zawierać słowa kluczowe (zawsze napisane wielkimi literami), które określają stopień konieczności spełnienia wymagania. Zwroty MUST, MAY, SHOULD oraz ich formy zaprzeczone, pisane wielkimi literami są używane zgodnie z ich definicją określoną w RFC 2119.

Poniższa tabela przedstawia możliwe poziomy rekomendacji wraz z ich polskimi odpowiednikami.

RFC 2119	MUST	SHOULD	MAY	SHOULD NOT	MUST NOT
Odpowiednik	WYMAGANE	ZALECANE	OPCJONALNIE	NIE ZALECANE	ZABRONIONE

Zawsze, kiedy to możliwe, wymagania hardeningu przedstawione są w ujęciu szczegółowym. Wymagania mogą mieć także charakter ogólny wówczas, gdy omawiają zależności z innymi usługami Azure lub zewnętrznymi komponentami IT, nieomawianymi w niniejszym dokumencie.



04
Słownik pojęć

4 Słownik pojęć

Środowisko Container Apps (Container Apps Environment) - stanowi bezpieczną granicę wokół grup aplikacji kontenerowych, które współdzielą tę samą sieć wirtualną i zapisują logi do tego samego miejsca docelowego.

po więcej szczegółów skontaktuj się z naszym konsultantem

05 Wymagania hardeningu

5 Wymagania hardeningu – legenda

REF

numeracja referencji hardeningu usługi

opis wymagania

krótki opis danej referencji

sposób realizacji

rozwinięcie opisu danej referencji wraz z uzasadnieniem oraz często z odniesieniami do dokumentacji

poziom wymagania

stopień konieczności spełnienia wymagania (opis poziomów znajduje się w rozdziale nr 3)

TF kod Terraform

informacja czy dana referencja jest możliwa do skonfigurowania w kodzie Terraform usługi

5.1 Architektura i integralność danych

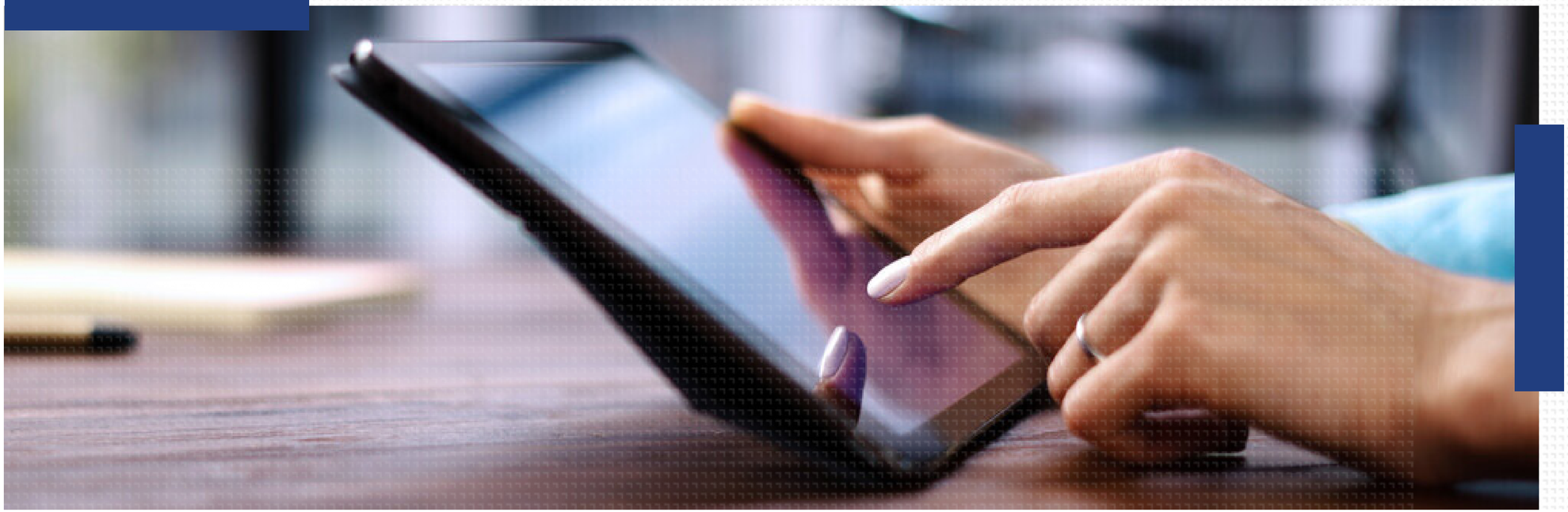
REF	opis wymagania	sposób realizacji	poziom wymagania	TF
5.1.01	Korzystanie z prywatnego repozytorium obrazów w usłudze Microsoft Azure Container Registry z uwierzytelnieniem poprzez tożsamość zarządzaną	Usługa Azure Container Apps wspiera dwa źródła do importowania obrazów kontenerowych – Azure Marketplace z predefiniowanymi obrazami oraz prywatne repozytoria Microsoft Azure Container Registry z obrazami skonfigurowanymi przez użytkownika. Zalecanym źródłem jest prywatne repozytorium, możliwe jest jednak dopuszczenie obrazów z Azure Marketplace, jeśli konsument nie konfiguruje własnych obrazów. W celu uwierzytelnienia w serwisie wymagane jest użycie tożsamości zarządzanych, by uniknąć używania poświadczeń administracyjnych. Dodatkowo, ruch sieciowy do prywatnego repozytorium obrazów powinien być zabezpieczony. W tym celu zalecane jest w repozytorium stworzenie private endpointów ze wskazaniem na podsieci, w których tworzone są środowiska aplikacji oraz ograniczenie publicznego dostępu jedynie do tych sieci.	**SHOULD**	**TAK**
5.1.02	Wdrażanie zasobów w procesie CI/CD z wykorzystaniem Azure Pipelines	Rozwiązania oparte na Azure Pipelines polegają na wykorzystaniu repozytorium Azure DevOps, w którym przechowywany jest kod aplikacji. Następnie, na skutek commitów nowych wersji kodu do odpowiedniego brancha, aktualizowany jest obraz kontenera w rejestrze kontenerów. Wówczas zasób Azure Container Apps tworzy nową rewizję bazując na zaktualizowanym obrazie. https://learn.microsoft.com/en-gb/azure/container-apps/azure-pipelines	**MAY**	**N/D**

5.1.03	Wykorzystywanie Azure Files Share jako stałego magazynu, w szczególności w przypadku korzystania z dużych plików w aplikacjach	W celu montowania udziałów do kontenerów aplikacji (a w szczególności w momencie wykorzystywania dużych plików) wymagane jest wykorzystanie Azure Files w wersji Premium jako stałego magazynu (volume share). Wersja Premium jest zalecana w przypadku obciążeń, które wymagają szybkiego stałego przechowywania i wielu równoczesnych małych losowych odczytów/zapisów. https://techcommunity.microsoft.com/t5/fasttrack-for-azure/azure-container-apps-working-with-storage/ba-p/3561853 W tym celu należy zadbać również o konfigurację usługi Azure Storage pod kątem bezpieczeństwa (tj. wyłączyć przestarzałe algorytmy kryptograficzne oraz protokoły, wymusić użycie szyfrowania at rest oraz in transit), np.: • Włączyć funkcję require secure transfer dla konta storage • Wyłączyć SMB < 3.0 • Wyłączyć dostęp publiczny (public network access) zaś umożliwić dostęp poprzez private endpoint (umiejscowienie storage account w prywatnej sieci wirtualnej) Powyższe, jak i inne rekomendacje bezpieczeństwa konfiguracji usługi Azure Storage powinny znajdować się w hardeningu usługi Azure Storage Account (poza zakresem tego dokumentu). https://learn.microsoft.com/en-us/azure/container-apps/storage-mounts?pivots=azure-cli#azure-files	**MUST**	**TAK**
5.1.04	Wybór rodzaju architektury sieciowej środowiska Consumption only zamiast Workload profiles	**Dostępne są dwa rodzaje architektury dla usługi Azure Container Apps:** • **Workload profiles environment (wersja preview) –** architektura wspierająca funkcję UDR (user defined routes) oraz ruch wychodzący poprzez NAT Gateway. Minimalny wymagany rozmiar podsieci wynosi w tym przypadku /27. W tym przypadku usługa rezerwuje 11 adresów IP w celu integracji z podsiecią. W przeciwieństwie do architektury Consumption only w przypadku korzystania z opcji Dedicated workload profile liczba wymaganych adresów IP nie zależy od skalowania środowiska aplikacyjnego – adresy IP przypisywane są per węzeł (ang. node); • **Consumption only environment –** podstawowy rodzaj architektury dla usługi, z minimalnym wymaganym rozmiarem podsieci wynoszącym /23. W tym przypadku usługa rezerwuje minimum 60 adresów IP w sieci wirtualnej, zaś liczba ta może wzrosnąć do 256 w przypadku skalowania środowiska aplikacyjnego (nowy adres IP jest przypisywany dla każdej nowo utworzonej repliki). **Z powodu wersji preview dla pierwszego typu architektury zalecanym rodzajem architektury jest Consumption only environment.**	**SHOULD**	**NIE**
		po więcej szczegółów skontaktuj się z naszym konsultantem		

5.2 Uwierzytelnienie i autoryzacja

REF	opis wymagania	sposób realizacji	poziom wymagania	TF
5.2.01	Wykorzystanie Managed Identities zamiast Service Principals	W celu konfiguracji usługi należy wybrać tożsamość, za pomocą której będą dokonywane operacje. Zaleca się wykorzystanie Azure Managed Identity zamiast Service Principal. Dane uwierzytelniające tożsamości Managed Identity są w pełni zarządzane, rotowane oraz chronione poprzez platformę Azure. Takie podejście powstrzymuje możliwość zapisania danych uwierzytelniających w kodzie źródłowym oraz plikach konfiguracyjnych. **Uwaga! Obecnie tożsamość zarządzana jest obsługiwana tylko dla komponentów Container Apps oraz Dapr. Nie jest zaś obsługiwana dla reguł skalowania w Container Apps.**	**SHOLULD**	**TAK**
5.2.02	Stworzenie ról dających minimalne poziomy dostępów	Rekomenduje się stworzenie ról dających szczegółowe uprawnienia do tworzenia i konfiguracji Azure Container Apps, monitorowania procesów, ale odbierających uprawnienia do definiowana i modyfikowania usług powiązanych. Rekomenduje się rozdzielenie ról deployera oraz wsparcia technicznego. Należy stosować zasadę przyznawania minimalnych koniecznych uprawnień potrzebnych do realizacji zadania. Jako przykład mogą posłużyć następujące role: • **ContainerApps Deployer [custom] –** rola uprzywilejowana pozwalająca na niektóre modyfikacje konfiguracji bez możliwości zmiany uruchomionego oprogramowania • **ContainerApps Support [custom] –** rola dająca wyłącznie prawa odczytu konfiguracji Nie rekomenduje się przypisywania dedykowanej roli ContainerApp Reader kontom użytkowników, z powodu zbyt szerokich uprawnień do odczytu. Dla usługi nie istnieją inne predefiniowane role. Zarządzanie definicjami ról musi być scentralizowane i posiadać proces aktualizacji wraz ze zmianami w usłudze.	**MUST**	**TAK**

5.2.03	Dostarczanie certyfikatów klienckich	Wymaganym podejściem bezpieczeństwa jest szyfrowanie połączenia klient-aplikacja (jeśli to możliwe), szczególnie w przypadku wykorzystywania danych wrażliwych w środowisku. Usługa Azure Container Apps umożliwia dwustronne uwierzytelnienie mTLS. Certyfikat klienta umieszczany jest w środowisku aplikacji w specjalnie przeznaczonej do tego przestrzeni (która jest zarządzana wyłącznie przez platformę). https://learn.microsoft.com/en-us/azure/container-apps/client-certificate-authorization	**MUST**	**TAK**
		po więcej szczegółów skontaktuj się z naszym konsultantem		



5.3 Bezpieczeństwo komunikacji

REF	opis wymagania	sposób realizacji	poziom wymagania	TF
5.3.01	Zapewnienie szyfrowania danych in transit	Szyfrowanie danych w przesyle jest uwarunkowaniem koniecznym w przypadku konfigurowania usługi. W tym celu należy wymusić włączenie protokołu HTTPS oraz TLS w wersji v1.2 (i późniejszych) na wszystkich aplikacjach oraz serwisach internetowych.	**MUST**	**N/D**
5.3.02	Konfiguracja opcji HTTPS/TCP ingress	W przypadku, gdy aplikacja potrzebuje punktu końcowego HTTP lub TCP należy włączyć opcję Ingress usługi Container Apps z następującymi parametrami: • ruch limitowany wyłącznie do własnej sieci wirtualnej w Azure lub wyłącznie do środowiska aplikacji, gdy niepotrzebny jest ruch na zewnątrz aplikacji; • protokół HTTPS lub TCP. https://learn.microsoft.com/en-us/azure/container-apps/ingress?tabs=bash	**MUST**	**TAK**
5.3.03	Balansowanie ruchu ingress w związku z nowymi wersjami skonteneryzowanych aplikacji	Użycie balansowania ruchu pomiędzy rewizjami jest przydatne przy nowych wydaniach aplikacji, gdy istnieje potrzeba wykonania testów A/B albo weryfikacji stabilności i bezbłędnego działania nowych wydań. Z punktu widzenia bezpieczeństwa obydwa typy rewizji są dopuszczalne: single i multiple, adekwatnie do potrzeb. Jednakże należy pamiętać, że mechanizm rewizji nie służy do balansowania ruchu do tych samych wersji aplikacji, ale do wprowadzania nowych wersji aplikacji w sposób zrównoważony, dający możliwość szybkiego wycofania błędnie działającego wydania. W związku z tym nowe rewizje NIE powinny otrzymywać więcej ruchu niż poprzednie ich wersje, dopóki nie ma potwierdzonej testami pewności stabilności ich działania. https://learn.microsoft.com/en-us/azure/container-apps/revisions	**MAY**	**NIE**
		po więcej szczegółów skontaktuj się z naszym konsultantem		

5.4 Szyfrowanie danych at rest

REF	opis wymagania	sposób realizacji	poziom wymagania	TF
5.4.01	Szyfrowanie danych w spoczynku z wykorzystaniem Azure Files i CMK	Dane at rest, w przypadku korzystania z magazynu tymczasowego lub magazynu efemerycznego, są szyfrowane z wykorzystaniem kluczy zarządzanych przez Microsoft. Nie ma możliwości szyfrowania ich z wykorzystaniem kluczy klienckich (CMK). W przypadku wykorzystywania danych prawnie chronionych zabronione jest więc przechowywanie ich za pomocą tych dwóch magazynów, jedyną dostępną opcją jest tu magazyn Azure Files (szyfrowany za pomocą CMK).	**MUST**	**N/D**
5.4.02	Nieumieszczanie sekretów oraz wrażliwych danych konfiguracyjnych bezpośrednio w kodzie	Usługa Azure Container Apps posiada funkcję tworzenia sekretów jako par klucz/wartość w celu ochrony wrażliwych parametrów konfiguracyjnych. Dane te, np. hasła, łańcuchy połączeń itp., domyślnie są używane w rewizjach aplikacji bez odpowiedniego zabezpieczenia (tj. hardkodowane w kodzie), **co jest zabronione z punktu widzenia bezpieczeństwa.**	**MUST NOT**	**TAK**
		po więcej szczegółów skontaktuj się z naszym konsultantem		

5.5 Monitorowanie zdarzeń

REF	opis wymagania	sposób realizacji	poziom wymagania	TF
5.5.01	Włączenie zapisu i eksportu logów	W domyślnym wdrożeniu serwisu Azure Container Apps do wyboru użytkownika istnieją 3 opcje zarządzania logami: • eksport do usługi Log Analytics workspace; • eksport do usługi Azure Monitor (wersja preview); • brak eksportu oraz zapisywania logów, możliwość podglądu logów wyłącznie w czasie rzeczywistym. Wymaganym ustawieniem z punktu widzenia bezpieczeństwa jest konfiguracja eksportu logów w celu monitorowania usług oraz możliwości reagowania w czasie rzeczywistym na zaistniałe incydenty. W zależności od sposobu zarządzania logami do wyboru są dwie opcje eksportu, zaś tylko eksport do usługi Log Analytics workspace jest w wersji ogólnej dostępności (eng. GA - general availability).	MUST	TAK
		po więcej szczegółów skontaktuj się z naszym konsultantem		

5.6 Ciągłość działania

REF	opis wymagania	sposób realizacji	poziom wymagania	TF
5.6.01	Włączenie redundancji w obrębie regionu podczas konfiguracji środowiska Container Apps	W momencie inicjalnej konfiguracji Container Apps Environment rekomenduje się włączenie opcji redundancji w obrębie regionu. Jest to jedyny moment, w którym można skonfigurować to ustawienie. Po stworzeniu środowiska nie ma możliwości zmiany. Dzięki włączonej redundancji repliki aplikacji są automatycznie losowo rozmieszczane w strefach w regionie. Ruch jest dystrybuowany pomiędzy replikami, bazując na aktualnym obciążeniu. Jeśli nastąpi awaria strefy, ruch zostanie automatycznie przekierowany do replik w pozostałych strefach.	MUST	TAK
5.6.02	Ochrona przed przypadkowym skasowaniem za pomocą Management Lock	W celu dodatkowej ochrony zasobów przed przypadkowym lub niepożądanym usunięciem zalecane jest włączenie blokady przed usunięciem na poziomie zasobów.	SHOULD	TAK
		po więcej szczegółów skontaktuj się z naszym konsultantem		

Shaping the future of digital business

gft.com/pl

contact.poland@gft.com

gft.com/pl/pl/technology/thought-leadership

twitter.com/gft_polska

linkedin.com/company/gft-group

facebook.com/gftpolska