# Zarządzanie zmianami

Wiele organizacji ma pewnego rodzaju funkcjonalność *zarządzania zmianami*. W najprostszej formie zarządzanie zmianami powinno gwarantować, że zmiany zostaną wprowadzone dopiero po ich zatwierdzeniu, a ocena ryzyka ich wprowadzenia została poddana ocenie.

Zarządzanie zmianami może być przydatne w zarządzaniu podatnościami, pozwalając upewnić się, że proponowane zmiany nie przyczynią się do wprowadzenia nowych podatności na zagrożenia do systemu. Jednocześnie, w przypadku nieprawidłowego wykonania, zarządzanie zmianami może również utrudniać zarządzanie podatnościami i przyczyniać się do zwiększania ogólnego ryzyka przez spowolnienie zmian niezbędnych do usunięcia tych podatności.

Jak zostało to omówione w tym rozdziale, niektóre nowe technologie środowisk w chmurze mogą przyczyniać się do zmniejszenia ryzyka całkowitego wyłączenia tak, że przy mniejszym udziale ręcznego zarządzania zmianami możliwe jest osiągnięcie tego samego poziomu ryzyka operacyjnego. Część ogólnego programu zarządzania podatnościami na zagrożenia w chmurze może wpływać na modyfikację procesów zarządzania zmianami.

Na przykład przekazywanie nowego kodu wraz z poprawkami zabezpieczeń do produkcji może być normalnym działaniem, automatycznie zatwierdzanym przez zespół kontroli zmian, pod warunkiem istnienia zademonstrowanego procesu szybkiego powrotu do prawidłowego stanu. Może to zostać osiągnięte przez kolejną aktualizację, doprowadzającą do przywrócenia poprzedniej wersji lub przez wyłączenie ruchu do nowej wersji aplikacji, aż do momentu rozwiązania problemu. Jednakże większe zmiany, takie jak zmiany w projekcie aplikacji, mogą nadal wymagać przejścia do ręcznego procesu zarządzania zmianami.

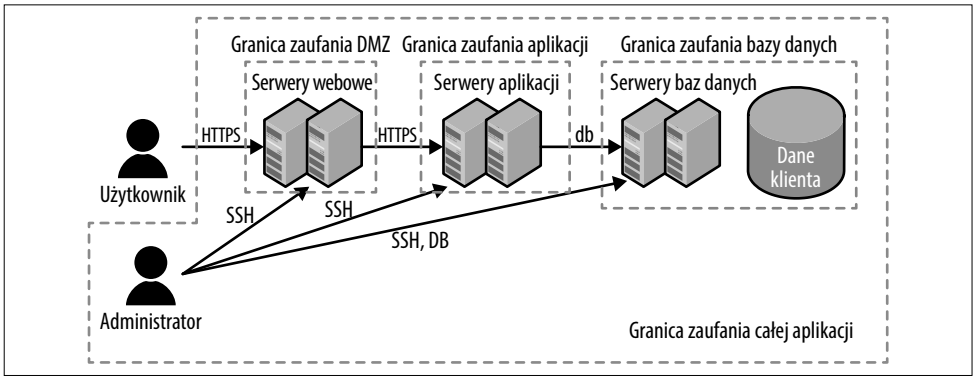
W idealnym przypadku w procesie kontroli zmian powinien brać udział co najmniej jeden specjalista do spraw bezpieczeństwa, zaangażowany jako członek zespołu kontroli zmian, ewentualnie jako doradca.

Udokumentowany proces zarządzania zmianami jest wymagany w przypadku szeregu certyfikatów przemysłowych i regulacyjnych, w tym SOC 2, ISO 27001 i PCI DSS.

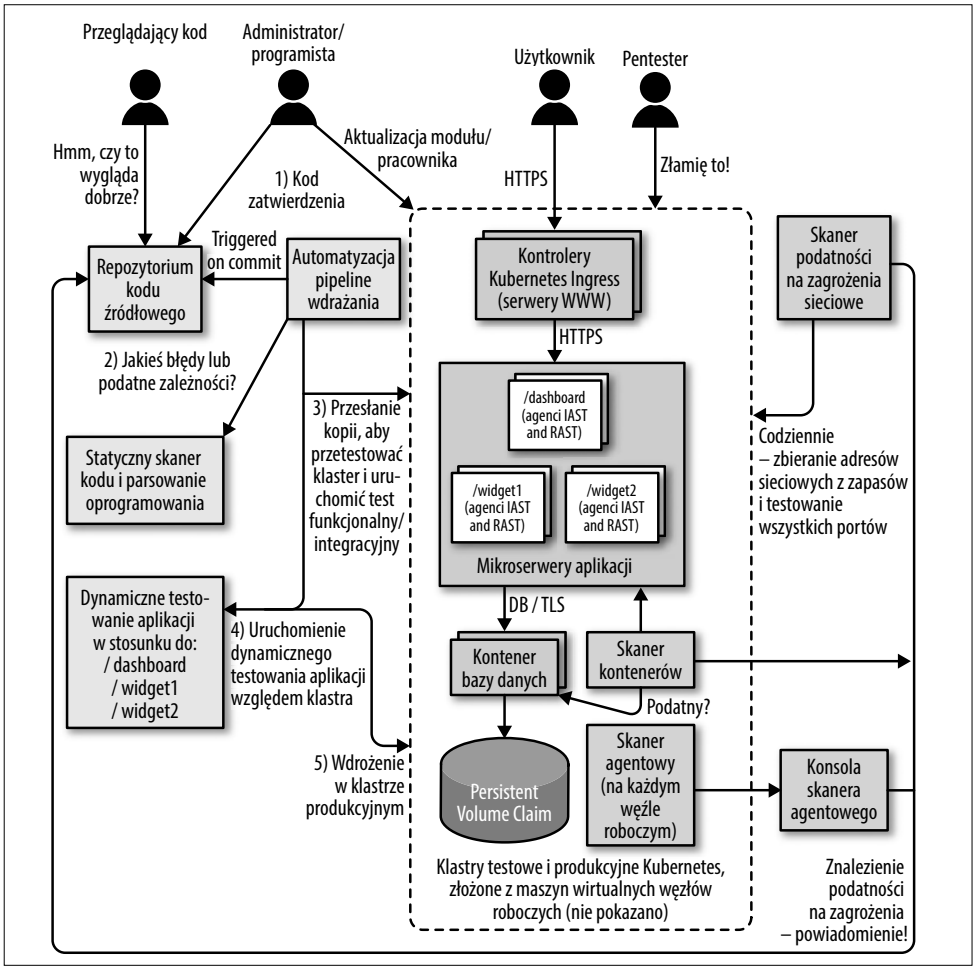
# Połączenie wszystkiego w przykładowej aplikacji

Na rysunku 5.3 przedstawiono przykładową, naprawdę prostą, trójwarstwową aplikację z rozdziału 1.

W przypadku zorganizowanego środowiska mikrousług opartych na kontenerach z testowymi i produkcyjnymi klastrami Kubernetes, przykładowa aplikacja może wyglądać nieco inaczej. Jednakże nadal możliwe jest wyodrębnienie tych samych, trzech głównych poziomów na środku schematu (rysunek 5.4).




*Rysunek 5.3. Schemat przykładowej aplikacji*




*Rysunek 5.4. Schemat przykładowej aplikacji w architekturze mikrousług*