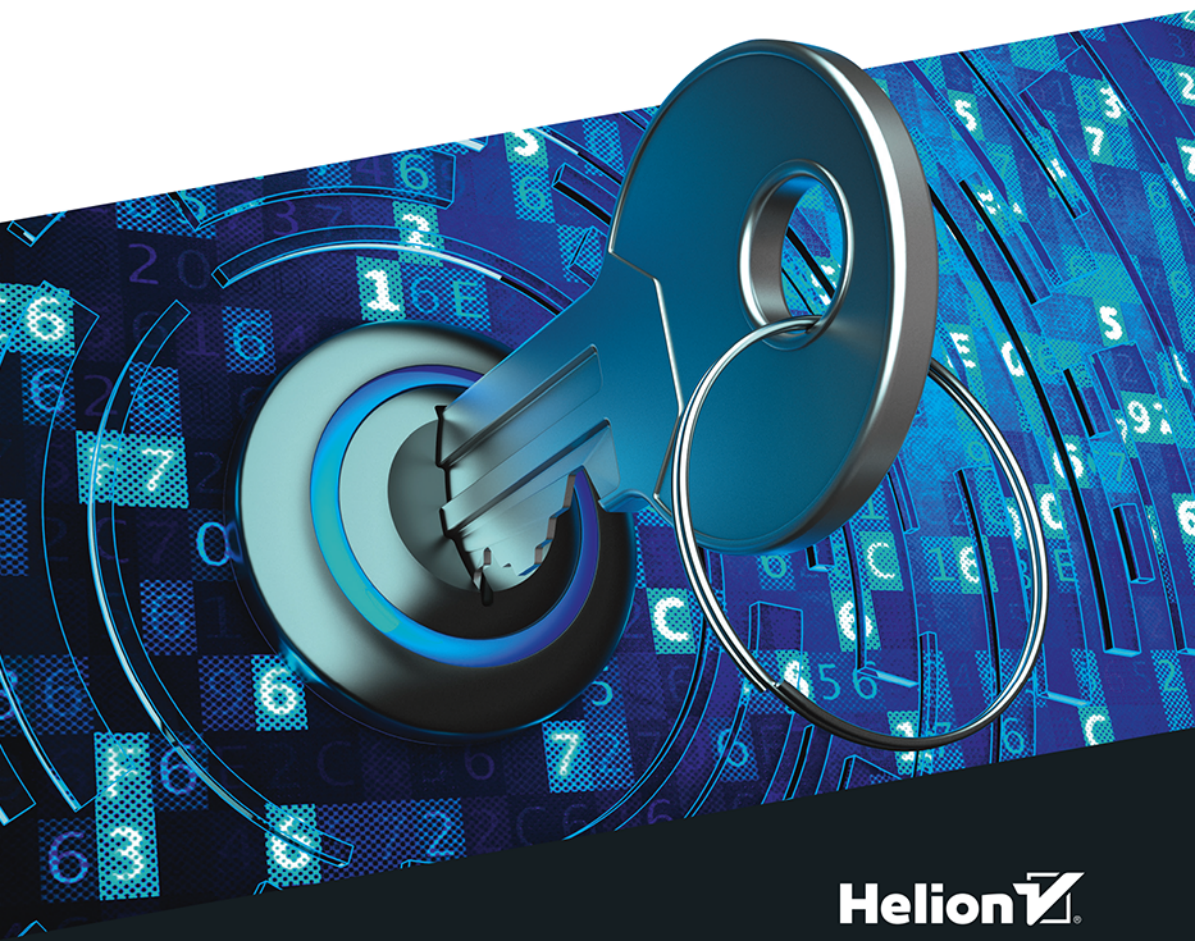
Dariusz Nabywaniec

# ANONIMIZACJA I MASKOWANIE danych wrażliwych w przedsiębiorstwach



Helion

Redaktor prowadzący: Małgorzata Kulik

Projekt okładki: Studio Gravite / Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Grafika na okładce została wykorzystana za zgodą Shutterstock.com

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
*http://helion.pl/user/opinie/anomas*
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-283-4495-2



Printed in Poland.

# Spis treści

# Chmury (Cloud Computing) a anonimizacja danych

Temat chmur z powodzeniem wykorzystuje się w zastosowaniach prywatności danych, której anonimizacja danych wrażliwych jest częścią. Przemyślana i dogłębnie zanalizowana zasadność użycia i dostosowanie zastosowania chmur do potrzeb naszego przedsiębiorstwa mogą znacząco obniżyć czas konfiguracji, uruchomienia i konserwacji struktury danych, a tym samym obniżyć koszt działania IT w naszym przedsiębiorstwie. Często rozwiązania chmurowe nie tylko obniżają koszt, lecz także są dodatkowym zabezpieczeniem danych wrażliwych stosowanych podczas anonimizacji. Nie oznacza to, że my też musimy koniecznie korzystać z chmury tylko dlatego, że inni z niej korzystają.

## Dla kogo jakie rozwiązania?

W przypadku średnich lub dużych przedsiębiorstw, które planują wdrożenie systemu chmurowego, skorzystanie z gotowych, prekonfigurowanych rozwiązań nie zawsze jest uzasadnione, bo z natury ogranicza możliwość dopasowania ich do indywidualnych wymagań. Jednocześnie jednak integracja elementów pochodzących od różnych producentów może być trudna i kosztowna, co czyni ją jednym z czynników zagrożeń.

Wyróżniane są następujące rodzaje chmur stosowanych przy anonimizacji danych:

**Chmura prywatna.** Jest obecnie najczęściej wykorzystywana w dużych firmach lub w przedsiębiorstwach, które podlegają szczególnie rygorystycznym i surowym regulacjom prawnym lub wymagają wysokiego bezpieczeństwa. Rozwiązanie typu chmura prywatna oznacza inwestycję we własny system IT, często przydzielenie czasu na konfigurację, a nawet zatrudnienie dodatkowego członka zespołu IT. Ostatecznie może więc to być wydatek podobny do wydatku na budowę klasycznego centrum danych lub wynajęcie odpowiednio zabezpieczonej, izolowanej infrastruktury zewnętrznej. Użytkownik zyskuje możliwość łatwego dopasowywania wydajności aplikacji przy zmieniających się obciążeniach, a także szybkiego wdrażania nowego oprogramowania lub nowych usług. Jedną z możliwości zmniejszenia kosztów takiego systemu w wersji usług zewnętrznych są prywatne chmury współdzielone (ang. *Community Cloud*). W tym wypadku kilka firm o porównywalnych wymaganiach co do funkcji i zabezpieczenia systemu wykorzystuje izolowane pule zasobów o podobnej konfiguracji. Pozwala to na obniżenie kosztów przez przynajmniej częściowe skorzystanie z efektu skali.

**Chmura publiczna.** Jest najtańszym rozwiązaniem, jeśli wewnętrzne zasady bezpieczeństwa i przepisy prawne nie stawiają naszemu przedsiębiorstwu żadnych szczególnych wymagań. Szybkie uruchamianie usług jest ważne dla rozwoju biznesu, a jednocześnie nie ma potrzeby integracji z funkcjami innych działów przedsiębiorstwa. Najczęściej niemal natychmiast po zarejestrowaniu w portalu usługodawcy i wniesieniu odpowiednich opłat nasze przedsiębiorstwo może uzyskać dostęp do wymaganej pamięci masowej i usług prekonfigurowanych dla anonimizacji danych. Rozwiązanie takie ma też wady. Na przykład duże firmy świadczące usługi masowe z reguły oferują standardowy zakres funkcji dopasowanych do wymagań przeciętnego odbiorcy. Jeśli nie spełniają one potrzeb użytkownika, to względnie niskie koszty usługi tracą znaczenie.

**Chmury hybrydowe.** Metoda ta łączy w jednym systemie funkcje chmur prywatnych i publicznych. Umożliwia ona uruchamianie aplikacji w systemie prywatnym, a przy okresowych, dużych wzrostach obciążenia wspomaga działanie systemu przy użyciu chmury publicznej. Innym rozwiązaniem hybrydowym jest wdrożenie systemu, w którym obsługa najważniejszych, krytycznych lub wymagających szczególnie wysokiego poziomu bezpieczeństwa aplikacji jest realizowana przez chmurę prywatną, a obsługa innych, mniej ważnych — przez publiczną. Metoda ta jest oczywiście połączeniem wszystkich zalet chmury publicznej i chmury prywatnej, ale zarazem połączeniem ich wszystkich wad.

**Ważne:** Jeśli Twoje przedsiębiorstwo potrzebuje elastyczności infrastruktury, a nie posiadasz funduszy na chmurę prywatną, wybierz chmurę publiczną.

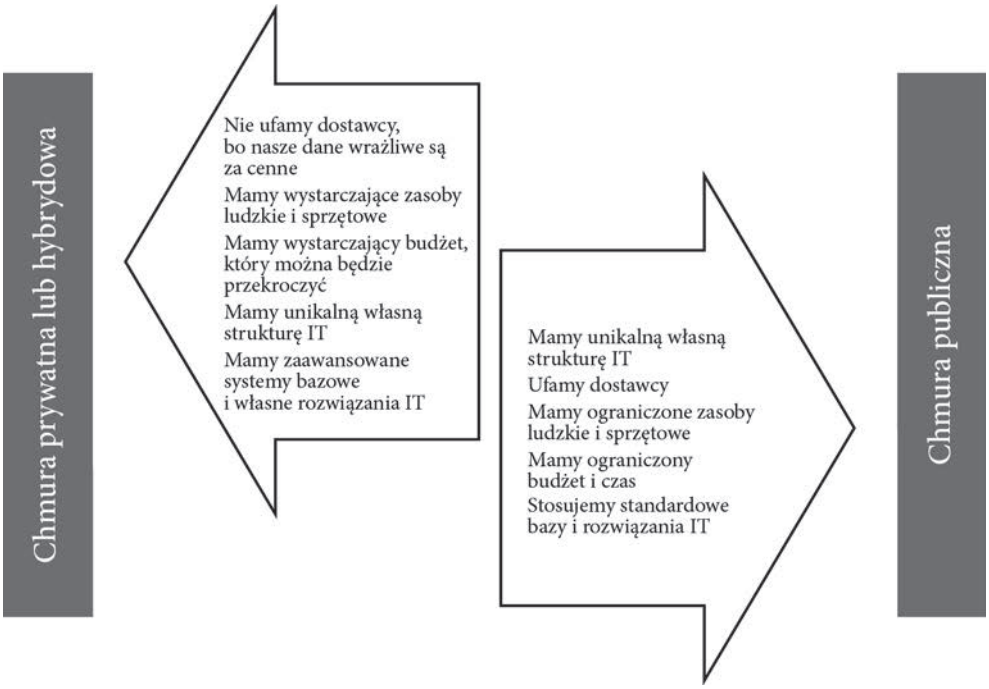
Korzyści wynikające ze stosowania chmur publicznych i hybrydowych:

- **Wydajność.** Jedną z największych zalet danych w chmurze jest wydajność. Wielkie centra obliczeniowe oferują moc nieosiągalną dla średnich lub małych przedsiębiorstw. Nie bez znaczenia jest też wzrost szybkości przetwarzania danych, wynikający ze skalowania i dynamicznego przydzielania zasobów. To, że wzrost obciążenia nie powoduje przestojów związanych z wydajnością, również przekłada się na efektywność działania danej firmy.
- **Łatwa skalowalność.** *Data Analyst*, DBA lub inni użytkownicy na pewno docenią swobodę i pozytywne aspekty dynamicznego przydzielania zasobów, gdy tylko okaże się, że są potrzebne. Dzięki temu nie trzeba płacić za utrzymanie infrastruktury „na wszelki wypadek". Oczywiście za wykorzystaną dodatkową moc obliczeniową chmury czy obsługę większej liczby transakcji trzeba zapłacić, ale jest to element bardzo dynamiczny.
- **Dostępność.** Dane są dostępne w chmurze z każdego komputera podłączonego do internetu. W tradycyjnym modelu korzystania z aplikacji instalowanych na stanowiskach pracy i licencjonowanych zależnie od ich liczby uzyskanie podobnej funkcjonalności jest trudne, a czasami wręcz niemożliwe. Warto też pamiętać o tym, że w przypadku usług w chmurze użytkownik nie musi się martwić o to, czy sprzęt, z którego korzysta, ma odpowiednią wydajność.

- **Transparentność i łatwość zarządzania.** Przedsiębiorstwo korzystające z kompleksowego zestawu narzędzi do anonimizacji w chmurze może nimi zarządzać za pomocą jasno i przejrzyście zdefiniowanego w obsłudze oprogramowania i najczęściej spójnego panelu administracyjnego, z którego można zarządzać całą funkcjonalnością. Nie ma potrzeby tworzenia dodatkowych różnych poziomów administracyjnych do zarządzania danymi, ponieważ elementy te są już od razu zdefiniowane i przygotowane przez dostawcę oprogramowania. Do użytkownika chmury trafiają po prostu łatwo zarządzane instancje narzędzi do anonimizacji, a to, w jaki sposób są one fizycznie zorganizowane, nie ma dla naszego przedsiębiorstwa żadnego znaczenia.
- **Elastyczność.** Zamiast kupować nowe serwery, dbać o ich prawidłową konfigurację, zgodność z istniejącymi rozwiązaniami itp., można skorzystać z gotowych usług oferowanych przez dostawców narzędzi do anonimizacji w chmurze.
- **Niezawodność.** Budowanie bezpiecznej infrastruktury zapewniającej nieprzerwane działanie może być wyzwaniem nawet dla dużego przedsiębiorstwa. Dostawcy usług w chmurze bardzo podkreślają niezawodność infrastruktury swoich centrów danych — jest ona nie tylko zaletą, ale także koniecznością, bo warunkuje sukces biznesowy inwestycji. W tradycyjnym modelu korzystania z danych jednego serwera lub kilku serwerów lokalnych awaria zmniejsza ogólną wydajność, a tym samym zmniejsza niezawodność. W chmurze ze względu na idee nie ma czegoś takiego jak awaria serwera danych, a nawet jeśli następuje jakaś awaria, zadania jednego serwera realizowane są przez inne maszyny.
- **Ekologia.** Efektywniejsze wykorzystanie mocy obliczeniowej i przestrzeni na dane przekłada się na mniejsze zużycie zasobów naturalnych energii, a tym samym na koszt całkowity przedsiębiorstwa.

Korzyści wynikające ze stosowania chmur prywatnych:

- **Lepsze wykorzystanie mocy w naszym przedsiębiorstwie.** Tuning i wykorzystanie wydajności poprzez poprawnie dostosowany i skonfigurowany system zdefiniowany przez *Data Analyst*, DBA lub innych członków IT jest korzystny dla finansów każdego dużego przedsiębiorstwa, które w sposób zdefiniowany przez CPO/CDO nie może skorzystać z chmur publicznych.
- **Transparentność i łatwość zarządzania.** Przedsiębiorstwo korzystające z własnej chmury i posiadające zestaw narzędzi do anonimizacji w chmurze może nimi zarządzać za pomocą jasno i przejrzyście zdefiniowanego w obsłudze oprogramowania i najczęściej pojedynczego panelu administracyjnego, z którego można zarządzać całością. Dla chmur prywatnych lub hybrydowych nie ma potrzeby tworzenia dodatkowych różnych poziomów administracyjnych do zarządzania danymi, ponieważ elementy te są już od razu zdefiniowane i przygotowane przez dostawcę lub przez nas samych. Tutaj również do użytkownika chmury trafiają po prostu łatwo zarządzane instancje narzędzi do anonimizacji, a to, w jaki sposób są one fizycznie zorganizowane, zależy od własnych wymagań, najczęściej ustawionych jednorazowo przez administratorów, DBA lub innych członków działu IT.




*Wybór odpowiedniej chmury dostosowanej do możliwości naszego przedsiębiorstwa*

# Zaufanie do dostawcy rozwiązań Cloud Computing

Zaufanie do dostawcy jest tematem często pomijanym lub nawet ignorowanym przez przedsiębiorstwa, które chcą przeprowadzić wdrożenie rozwiązań IT. Jak bardzo powinniśmy zaufać dostawcy chmur, by nasze dane zawsze były bezpieczne? Czy dostawca gwarantuje takie rozwiązania, które pod względem prawnym zabezpieczą nas w momencie wycieku danych poufnych? Często informacje te należy poddać analizie, żeby stwierdzić, czego właściwie dana usługa dotyczy i jakie są gwarancje prawne w przypadku utraty danych wrażliwych. Ostateczne podjęcie decyzji powinno zostać przeanalizowane, przedyskutowane i należycie udokumentowane przez prawników, dział IT, CPO/CDO i zespół do spraw bezpieczeństwa lub ryzyka w naszym przedsiębiorstwie.

**Ważne:** Zaufanie do dostawcy powinno być zawsze ograniczone i poddawane ciągłym niezależnym audytom.

# Skorowidz

## K



## M



## N



## O



## P



## R

## S



## Ś



## T



## W



## Z

## Zostań ekspertem w zakresie anonimizacji wrażliwych danych!

- **Czym są dane wrażliwe?**
- **Jak je zabezpieczyć przed wyciekiem?**
- **Jak maskować dane i pozostać anonimowym w sieci?**

Współczesny świat produkuje ogromne ilości danych, z których duża część to dane wrażliwe. Ich wyciek poza przechowujące je przedsiębiorstwo czy instytucję nie tylko naraża na szwank reputację organizacji, lecz również niesie za sobą ryzyko konkretnych strat finansowych i poważne konsekwencje o charakterze prawnym. Aby nie dopuścić do tego rodzaju sytuacji, firmy na całym świecie odpowiednio się zabezpieczają, a składową tych działań jest anonimizacja danych, czyli takie ich przetwarzanie, dzięki któremu staną się bezwartościowe, gdy wpadną w niepowołane ręce.

*Anonimizacja i maskowanie danych wrażliwych w przedsiębiorstwach* to książka, dzięki której dowiesz się, jakie zagrożenia wiążą się z przechowywaniem poufnych danych, a także poznasz sposoby pozwalające ograniczyć wynikające z tego ryzyko. Na podstawie własnego doświadczenia i na praktycznych przykładach autor prezentuje najlepsze praktyki anonimizacji i maskowania danych, wykorzystywane w tym celu narzędzia i techniki oraz pułapki czyhające na firmy, które nie stosują właściwych zabezpieczeń.

To obowiązkowa lektura dla wszystkich osób odpowiedzialnych za bezpieczeństwo i zachowanie prywatności danych, administratorów baz danych, architektów oprogramowania, analityków danych i dyrektorów technicznych przedsiębiorstw z branży IT — a tak naprawdę dla każdego, kto zawodowo ma do czynienia z systemami informatycznymi przechowującymi i przetwarzającymi wrażliwe informacje. Przeczytaj, zanim będzie za późno!

- **Wyszukiwanie i rozpoznawanie danych wrażliwych**
- **Analiza ryzyka i sposoby zabezpieczania danych**
- **Role i obowiązki osób odpowiedzialnych za prywatność danych**
- **Narzędzia i metody stosowane w anonimizacji danych**
- **Techniki maskowania i szyfrowania danych**

## Zabezpiecz się zawczasu — anonimizuj poufne dane!

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl



ISBN 978-83-283-4495-2



Cena: 39,90 zł