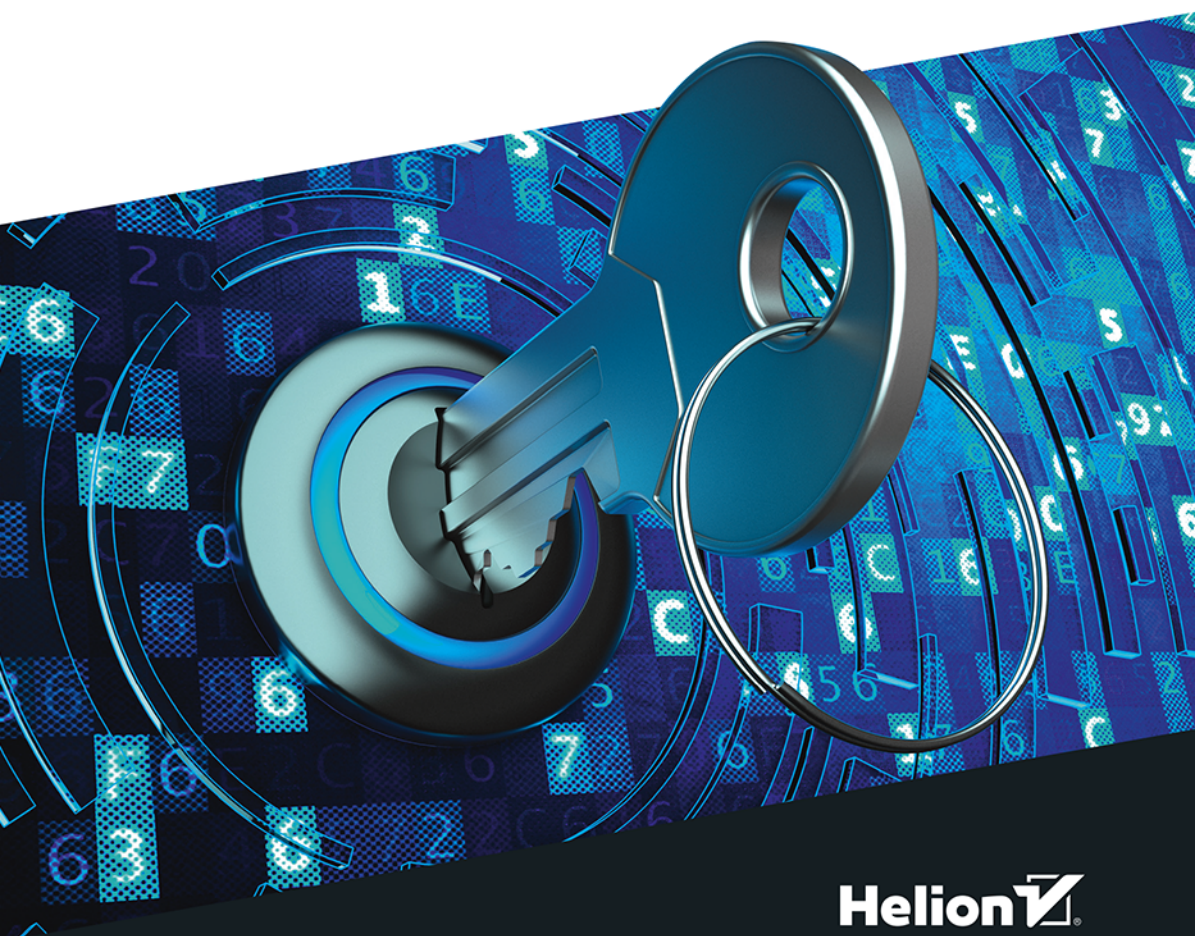


Dariusz Nabywaniec

ANONIMIZACJA I MASKOWANIE danych wrażliwych w przedsiębiorstwach



Helion 

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz Wydawnictwo HELION dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz Wydawnictwo HELION nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

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

Copyright © Helion 2019

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści

| | |
|---|-----------|
| O mnie i o książce | 9 |
| Początki anonimizacji danych w IT | 11 |
| Po co anonimizacja danych? | 12 |
| Do kogo skierowana jest anonimizacja danych? | 14 |
| Czym właściwie jest anonimizacja danych wrażliwych? | 18 |
| Stopień miary anonimizacji danych | 20 |
| Zrównoważenie przebiegu anonimizacji danych | 22 |
| Co to są dane wrażliwe? | 24 |
| TDM z perspektywy anonimizacji danych wrażliwych | 25 |
| Standardy stosowane dla danych wrażliwych | 26 |
| Definicja zespołu odpowiedzialnego za dane wrażliwe | 28 |
| Role i obowiązki CPO/CDO (z perspektywy danych wrażliwych) | 28 |
| Wizja i decyzyjność CPO/CDO | 29 |
| Role i obowiązki zespołu odpowiedzialnego za anonimizację w systemie ITSM | 29 |
| Zgłoszenie naruszenia wrażliwości danych poza systemem ITSM | 32 |
| Zgłoszenie naruszenia wrażliwości danych w systemie ITSM | 34 |
| Przeływ danych w systemie ITSM | 36 |
| Nie wiem, jakiego obszaru lub środowiska dotyczyło naruszenie | 36 |

| | |
|--|-----------|
| Znajdujemy dane wrażliwe — czy moje dane są wrażliwe? | 38 |
| Identyfikacja naszych danych wrażliwych | 38 |
| Kontekst wrażliwości danych | 39 |
| Anomalie danych — obsługa błędów i wyjątków | 39 |
| Analiza ryzyka a wycieki danych wrażliwych | 41 |
| Najczęstsze przyczyny wycieków danych wrażliwych | 42 |
| Eliminacja wycieków — praktyczne zastosowanie anonimizacji danych | 43 |
| Codzienna świadomość zagrożeń | 44 |
| Anonimizacja i autoryzacja dla koncepcji DCS | 45 |
| Dane skorelowane z polityką bezpieczeństwa | 46 |
| Metody znajdowania danych produkcyjnych | 50 |
| Metoda od dołu | 50 |
| Metoda big bang | 50 |
| Metoda obszarów | 50 |
| Rozpoczęcie projektu wdrożenia anonimizacji | 52 |
| Kroki i fazy projektu | 52 |
| Jak przydzielać zadania dotyczące maskowania danych wrażliwych? | 55 |
| Czym jest Złota Kopia bazy (Golden Copy)? | 57 |
| Złota Kopia — jak to się robi? | 57 |
| Najczęstsze problemy ze Złotą Kopią | 58 |
| Ile kosztuje pełna anonimizacja danych wrażliwych? | 59 |
| Kiedy będzie sukces? | 60 |
| Własne rozwiązania w zakresie anonimizacji danych wrażliwych | 61 |
| Wybór odpowiedniego narzędzia do anonimizacji danych | 62 |
| Różne typy baz wykorzystywanych w przedsiębiorstwie | 62 |
| Środowiska wykorzystujące jednego dostawcę SZBD | 62 |
| Środowiska wykorzystujące różnych dostawców SZBD | 63 |
| Lista dostawców narzędzi do anonimizacji | 63 |
| Wersja próbna / pilot narzędzia do anonimizacji | 65 |
| Nasze środowisko — atrybuty klasyfikacyjne | 66 |

| | |
|--|------------|
| Prototyp rozwiązania — POC (Proof of Concept) | 68 |
| Etapy procesu wyboru narzędzia do anonimizacji danych i wybór końcowy | 70 |
| Etap 1. — minimum założonych wymagań | 71 |
| Etap 2. — warunki techniczne | 72 |
| Zakres prac — SOW (Statement of Work) | 74 |
| Etap 3. — wybór końcowy narzędzia | 75 |
| Obsługa poprodukcyjna anonimizacji danych | 77 |
| Dlaczego nie możemy zrobić tego sami? | 79 |
| Najczęstsze pułapki związane z nieprawidłowym wyborem własnych rozwiązań | 80 |
| Kilka sposobów na porażkę przy wdrażaniu systemu anonimizacji | 81 |
| Poziomy anonimizacji w Twoim przedsiębiorstwie | 82 |
| Big data — coraz więcej danych! Coraz trudniej to ogarnąć! | 83 |
| Wzrost popularności nowych typów danych | 83 |
| Wzrost objętości danych | 84 |
| Chmury (Cloud Computing) a anonimizacja danych | 85 |
| Dla kogo jakie rozwiązania? | 85 |
| Zaufanie do dostawcy rozwiązań Cloud Computing | 88 |
| Miara poziomów zabezpieczeń danych wrażliwych | 89 |
| Dostosowanie modelu anonimizacji do potrzeb przedsiębiorstwa | 91 |
| Klasyfikacja anonimizacji danych wrażliwych | 93 |
| Przebieg analizy danych wrażliwych | 96 |
| Przydziel dostęp do bazy | 96 |
| Wyszukaj metadane | 97 |
| Automatyzuj wyszukiwanie danych wrażliwych | 98 |
| Ręczna analiza danych i wyszukiwanie wyjątków | 98 |
| Zatwierdzenie | 99 |
| Z czego się składa pełna anonimizacja danych? | 100 |
| Maskowanie statyczne jako proces anonimizacji danych wrażliwych | 102 |

| | |
|--|------------|
| Trzy warianty maskowania statycznego | 103 |
| Wariant 1. — statyczny EAL (Extract, Anonimize, Load) | 103 |
| Wariant 2. — statyczny ELA (Extract, Load, Anonimize) | 104 |
| Wariant 3. — statyczny podzbiór danych bez kopii bazy produkcyjnej | 105 |
| Przykład błędnego scenariusza | 105 |
| Przykład pozytywnego scenariusza | 105 |
| Wariant 3B — statyczny podzbiór danych kopii bazy produkcyjnej | 106 |
| Przykład błędnego scenariusza | 107 |
| Przykład pozytywnego scenariusza | 107 |
| Maskowanie dynamiczne jako proces anonimizacji danych wrażliwych | 107 |
| Zastosowania anonimizacji dynamicznej w przedsiębiorstwie | 109 |
| Formatowanie danych dla maskowania statycznego | 111 |
| | |
| Maskowanie danych — co to jest? | 113 |
| Prawa maskowania danych wrażliwych | 113 |
| Logiczna kolejność analizy maskowania danych | 115 |
| Stosowane techniki maskowania | 117 |
| Kroki milowe maskowania | 117 |
| Kroki milowe maskowania — podział na tygodnie | 118 |
| Kroki milowe maskowania — podział na aplikacje | 119 |
| Schemat maskowania danych standardowych | 119 |
| Maskowanie typów logicznych (tak/nie) | 119 |
| Maskowanie imion i nazwisk w języku polskim | 120 |
| Maskowanie pól daty | 121 |
| Maskowanie pól e-mail | 122 |
| Maskowanie pól adresu (jeśli nie jest ważna poprawność adresu) | 123 |
| Maskowanie przez podstawienie (bez aliasu) — Standard Substitution | 125 |
| Maskowanie przez podstawienie z aliasem — (Substitution Lookup) | 127 |
| Maskowanie przez szablon zmian | 130 |
| Maskowanie wyliczeniowe | 132 |
| Maskowanie wyliczeniowe (z argumentem progowym) | 133 |
| Maskowanie wyliczeniowe podsumowujące | 133 |
| Maskowanie z innymi parametrami | 134 |
| Maskowanie losowe (Shuffle) | 135 |
| Maskowanie a problem integralności logicznej danych | 136 |
| Ustalenie rozwiązań problemów integracyjnych | 136 |

| | |
|---|------------|
| Zastosowanie szyfrowania do anonimizacji danych | 140 |
| Techniki szyfrowania stosowane do anonimizacji danych | 140 |
| Ogólna idea szyfrowania danych | 140 |
| Techniki haszowania danych w anonimizacji danych | 142 |
| Testowanie danych zanonimizowanych i reakcja na błędy | 143 |
| Metoda Zero Absolutne | 143 |
| Metoda 1+ | 144 |
| Działanie algorytmów maskowania | 145 |
| Maskowanie dynamiczne na przykładzie Microsoft SQL Server 2016 | 146 |
| Maskowanie statyczne w IBM InfoSphere Optim (wersja 11.3) | 152 |
| Maskowanie statyczne w Ab Initio Express IT | 155 |
| Wbudowane funkcje maskujące | 155 |
| Kroki procesu maskowania danych w Ab Initio | 156 |
| Zasada działania maskowania danych w Ab Initio | 158 |
| Obsługa wyjątków i błędów poprzez stosowanie własnych wyrażeń maskujących | 160 |
| Reorganizacja danych a maskowanie danych | 161 |
| Shuffle Masking jako maskowanie losowe i maskowanie przez podstawienie | 162 |
| Subsetting Masking jako maskowanie wyliczeniowe i maskowanie szablonowe | 163 |
| Akronimy | 165 |
| Bibliografia | 169 |
| Skorowidz | 171 |

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 przejrzysto 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 przejrzysto 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

A

Ab Initio Express IT, 155
AES, Advanced Encryption Standard, 165
algorytmy maskowania, 145
analiza ryzyka, 41
anomalie danych, 39
anonimizacja danych, 12
 wrażliwych, 18
architektura SZBD, 62
atrzybuty klasyfikacyjne, 66
automatyzacja wyszukiwania, 98
autoryzacja, 45
 danych, 48

B

bazy danych, 62
bezpieczeństwo, 46
 danych, 46
Big data, 83, 165
błędy, 39, 160

C

CDO, Chief Data Officer, 28, 165
CEO, Chief Executive Officer, 165
chmura, Cloud Computing, 85, 165
chmury
 dostępność, 86
 elastyczność, 87
 hybrydowe, 86
 koszt, 87
 łatwość zarządzania, 87
 niezawodność, 87
 prywatne, 85
 publiczne, 86
 skalowalność, 86
 transparentność, 87

wydajność, 86

 zaufanie do dostawcy, 88

CPO, Chief Privacy Officer, 28, 165

D

dane
 produkcyjne, 50
 wrażliwe, 24, 26, 38
DCS, Data Centric Security, 45, 166
DDM, Dynamic Data Masking, 146
decyzyjność CPO/CDO, 29
dostawca
 narzędzi, 63
 rozwiązań Cloud Computing, 88
dostęp do bazy, 96
dostosowanie modelu do potrzeb, 91
działanie algorytmów maskowania, 145

E

eliminacja wycieków, 43

F

formatowanie danych, 111
funkcje maskujące, 155

H

haszowanie danych, 142
HIPAA, 26, 166

I

IBM InfoSphere Optim, 152
identyfikacja danych wrażliwych, 38
Internet rzeczy, IOT, 166
IOT, Internet of Things, 166

IT, Information Technology, 166

ITSM

- obowiązki zespołu, 29
- przepływ danych, 36
- role zespołu, 29
- zgłoszenie naruszenia wrażliwości danych, 34

ITSM, IT service management, 32, 166

K

klasyfikacja, 93

kontekst wrażliwości danych, 39

koszt całkowity anonimizacji, 59

M

maskowanie danych, 113

- dynamiczne, 107, 146

- integralność logiczna danych, 136

- kroki milowe, 117

- logiczna kolejność analizy, 115

- losowe, 135, 162

- prawa, 113

- przez podstawienie, 125, 162

- z aliasem, 127

- przez szablon zmian, 130

- schemat, 119

- statyczne, 102, 152, 155

- formatowanie danych, 111

- statyczny EAL, 103

- statyczny ELA, 104

- statyczny podzbiór danych, 105, 106

- szablonowe, 163

- techniki, 117

- w Ab Initio, 158

- wrażliwych, 55

- wyliczeniowe, 132, 163

metadane, 97

metoda

- 1+, 144

- big bang, 50

- obszarów, 50

- od dołu, 50

- Zero Absolutne, 143

MS SQL Server 2016, 146

N

naruszenie wrażliwości danych, 32, 34

narzędzia, 62, 63, 65

- wybór, 70

O

obowiązki

- CPO/CDO, 28

- zespołu, 29

obsługa

- błędów, 39, 160

- poprodukcyjna anonimizacji, 77

- wyjątków, 39, 160

P

PCI/DSS, Payment Card Industry Data Security Standard, 166

pełna anonimizacja danych, 59, 100

PGP, Pretty Good Privacy, 166

PHI, 26

PII, Personally Identifiable Information, 26

PII/PHI, 166

POC, Proof Of Concept, 68, 166

polityka bezpieczeństwa, 46

poziom

- anonimizacji, 82

- zabezpieczeń, 89

projekt wdrożenia anonimizacji, 52

- fazy, 52

- kroki, 52

przebieg analizy danych, 96

przepływ danych, 36

pułapki, 80

R

RDMS, Relational Database Management System, 136

reakcja na błędy, 143

reorganizacja danych, 161

ręczna analiza danych, 98

role

- CPO/CDO, 28

- zespołu, 29

S

SDLC, System Development Live Cycle, 166
 Shuffle Masking, 162
 SLA, Service Level Agreement, 167
 SOW, Statement of Work, 74, 167
 standard CI DSS, 11
 Standard Substitution, 125
 statyczny
 EAL, 103
 ELA, 104
 podzbiór danych, 105, 106
 stopień miary, 20
 Subsetting Masking, 163
 Substitution Lookup, 127
 system
 ITSM, 32, 34
 RDMS, 136
 SZBD, 62, 167
 szyfrowanie, 140
 techniki, 140

Ś

świadomość zagrożeń, 44

T

TDM, Test Data Management, 25
 techniki
 haszowania danych, 142
 szyfrowania, 140
 testowanie
 akceptacyjne, 167
 danych, 143
 integracyjne, 167
 przedprodukcyjne, 167
 regresyjne, 167
 wydajnościowe, 167

W

wdrażanie systemu anonimizacji, 15, 22, 52, 81
 własne rozwiązania, 61
 wybór
 narzędzi, 70
 własnych rozwiązań, 80
 wyciek danych wrażliwych, 41, 42
 wyjątki, 39, 160
 wyszukiwanie wyjątków, 98

Z

zachowanie prywatności danych, 15
 zagrożenia, 16, 44
 zakres prac, 74
 zatwierdzenie, 99
 zaufanie do dostawcy, 88
 zespół odpowiedzialny za anonimizację, 29
 zgłoszenie naruszenia wrażliwości danych, 32, 34
 Złota Kopia bazy, 57
 znajdowanie danych produkcyjnych, 50

PROGRAM PARTNERSKI

— GRUPY HELION —



1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA
Helion

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 zawnazas — anonimizuj poufne dane!

Helion 

 helion.pl

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

Sprawdź nasze szkolenia!

SZKOLENIA



AKADEMIA IT & BUSINESS

WWW.SZKOLENIA.HELION.PL

KOD KORZYŚCI
Sięgnij po więcej! ►



ISBN 978-83-283-4495-2



9 788328 344952