RAPORT

ANALIZA RYZYKA
dla bezpieczeństwa danych osobowych

Punkt Usługowy

Akceptuję

_____
Kierownictwo Organizacji

Spis treści:

1. Opis analizy ryzyka

W dokumencie przedstawiono wyniki procesu szacowania ryzyka dla bezpieczeństwa danych osobowych. W trakcie szacowania ryzyka przeprowadzono analizę ryzyka i ocenę ryzyka, czyli określono, które ryzyka są akceptowalne poprzez porównanie ich z wyznaczonym poziomem ryzyka, które można zaakceptować. W trakcie analizy ryzyka przeprowadzono identyfikację ryzyka i określono wielkości ryzyk.

Cechy informacji:
- Dostępność jest to właściwość określającą, że zasób jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony
- Integralności jest to właściwość określającą, że zasób nie został zmodyfikowany w sposób nieuprawniony.
- Poufności jest to właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym.

Zarządzanie ryzykiem
Proces zarządzania ryzykiem w prowadzi się w celu zapewnienia i utrzymania na poziomie akceptowanym przez kierownictwo organizacji bezpieczeństwa danych osobowych przetwarzanych w organizacji.
Zarządzanie ryzykiem składa się z następujących procesów:
- szacowanie ryzyka
- postępowanie z ryzykiem
- akceptacja ryzyka
- przegląd, monitorowanie i informowanie o ryzyku

Proces szacowania ryzyka składa się z:
- analizy ryzyka
- oceny ryzyka

Proces postępowania z ryzykiem:
- wybór sposobu działania z otrzymanym ryzykiem. Ryzyko możemy obniżyć wdrażając środki ochrony, pozostawić na wyliczonym poziomie, uniknąć ryzyka nie podejmując ryzykownych działań lub przenieść ryzyko na inny podmiot.

Proces akceptacji ryzyka:
- zatwierdzenie przez kierownictwo organizacji aktualnego stanu jako wystarczającego do ochrony danych osobowych.

Proces przeglądu, monitorowania i informowania o ryzyku:
- bieżąca analiza wdrożonych środków ochrony, otoczenia prawnego, środowiska eksploatacji systemu, zmian organizacji. Informowanie osób odpowiedzialnych za zarządzanie ryzykiem o zmianach ryzyka i nowych ryzykach

Szacowanie ryzyka

Szacowanie ryzyka jest to proces analizy ryzyka i oceny ryzyka. Analiza ryzyka jest to proces identyfikacji ryzyka i określenia wielkości ryzyk

Analiza ryzyka:
- identyfikacja aktywów, czyli informacje, osoby, usługi, oprogramowanie, dane i sprzęt, a także inne elementy mające wpływ na bezpieczeństwo informacji
- identyfikacja zagrożeń, czyli niepożądane zdarzenia, mogące mieć wpływ na dane osobowe
- identyfikacja podatności, czyli słabość zasobu lub zabezpieczenia , która może zostać wykorzystana przez zagrożenie
- identyfikacja zabezpieczeń, czyli środki o charakterze fizycznym, technicznym lub organizacyjnym
- identyfikacja skutków, czyli wyników działania zagrożenia
- określenie wielkości ryzyk, czyli wyznacza się poziomy zidentyfikowanych ryzyk

Ocena ryzyka:
- porównanie wyznaczonych poziomów ryzyk z tymi, które można zaakceptować. Na podstawie oceny podejmuje się decyzję co do dalszego postępowania z ryzykami

Szacowanie ryzyka przeprowadza się:
- przed podjęciem decyzji o wprowadzeniu niezbędnych zabezpieczeń
- w przypadku wprowadzania zmian, które mogą mieć wpływ na bezpieczeństwo informacji
- po wykryciu nowych zagrożeń lub zidentyfikowaniu nowych podatności, które nie były rozpatrywane podczas wcześniejszego szacowania ryzyka
- w przypadku zaistnienia istotnego incydentu bezpieczeństwa
- jeżeli zmianie lub rozszerzeniu uległo przeznaczenie, zadania lub funkcjonalność systemu
- okresowo, przy czym częstotliwość określa się w polityce bezpieczeństwa

Opis metodyki

Metodyka użyta w analizie ryzyka jest to metodyka jakościowa. W metodyce wartość ryzyka naruszenia bezpieczeństwa wyliczana jest jako iloczyn skutów działania zagrożenia (następstw) i prawdopodobieństwa tego zagrożenia.

RYZYKO = SKUTEK x PRAWDOPODOBIEŃSTWO

Na podstawie szacowania ryzyka dokonujemy wyboru środków ochrony, określamy zabezpieczenia które należy wdrożyć w celu zapewnienia ochrony danych osobowych. Szacowanie ryzyka pozwala zidentyfikować ryzyka naruszenia bezpieczeństwa, na jakie narażone są informacje przetwarzane w systemie, pozwala dobrać adekwatne zabezpieczenia, efektywnie chroniące zasoby, a przede wszystkim informacje składowane w tym systemie. Na podstawie szacowania ryzyka dokonujemy wyboru środków ochrony,

określamy zabezpieczenia które należy wdrożyć w celu zapewnienia ochrony danych osobowych.

Cel szacowania ryzyka:
- Określenie zagrożeń i podatności systemów na te zagrożenia
- Identyfikacja obszarów, dla których należy wdrożyć zabezpieczenia i środki zaradcze
- Określenie istniejącego ryzyka
- Określenie skuteczność istniejących zabezpieczeń
- Zgromadzenie informacji potrzebnych do wyboru efektywnych i niezbędnych zabezpieczeń

Przedstawiona metodyka określa ryzyka naruszenia bezpieczeństw na podstawie macierzy ryzyk. Macierz ryzyka obrazuje działania zagrożeń na zasoby. Działania te są opisane w postaci prawdopodobieństwa wystąpienia zagrożenia i skutków wystąpienia zagrożeń. Na podstawie prawdopodobieństwa i skutków otrzymujemy ryzyka. Każde ryzyko naruszenia bezpieczeństwa otrzymuje się z pary zasób i zagrożenie. Prawdopodobieństwa i skutki przedstawione są za pomocą skal liczbowych, a ich iloczyn stanowi ryzyko.

2. Dane projektu

Nazwa jednostki organizacyjnej: **Punkt Usługowy**

Opis systemu
Przykładowy opis projektu: Dane osobowe przetwarzane są na 4 komputerach stacjonarnych PC desktop. Wszystkie komputery znajdują się w pomieszczeniu zamykanym na klucz. W pomieszczeniu na stałe pracuje 4 pracowników, którzy sprawują nadzór w zakresie dostępu do pomieszczenia osób nieuprawnionych. Po godzinach pracy w pomieszczeniu uruchamiany jest system alarmowy, pomieszczenie posiada czujkę ruchu. Komputery mają zainstalowany system Windows 10 i podłączone są do Internetu. Windows 10 został skonfigurowany zgodnie ze standardami bezpieczeństwa m.in. każdy użytkownik posiada indywidualne konto w systemie, dostęp do systemu zabezpieczony jest hasłem 12 znakowym. Dane osobowe przchowywane są wyłącznie lokalnie na tych komputerach. Nie przechowuje się danych poza tymi komputerami...

3. Lista aktywów

Zasobem nazywamy informacje, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych informacji. W ramach identyfikacji ryzyka określono następujące zasoby.

Aktywa

Informacje
1. Dane osobowe na dysku twardym

Urządzenia stacjonarne
2. Komputer PC

Urządzenia peryferyjne
3. Drukarka

Nośniki elektroniczne
4. Dysk twardy

Inne nośniki
5. Wydruki papierowe

System operacyjny
6. Windows

Oprogramowanie standardowe
7. Pakiet biurowy office

Standardowe aplikacje biznesowe
8. Oprogramowanie do zarządzania klientami

Użytkownicy
9. Użytkownik

Personel ds. eksploatacji i utrzymania
10. Administrator systemu

Siedziba
11. Pomieszczenie

4. Lista zagrożeń

W ramach identyfikacji ryzyka określono zagrożenia. Poprzez zagrożenie należy rozumieć potencjalną przyczynę niepożądanego zdarzenia, które może wywołać szkodę w zasobach.

Naturalne
1. Pożar (naturalne)
2. Utrata dostaw prądu (naturalne)

Przypadkowe
3. Pożar (przypadkowe)
4. Awaria systemu klimatyzacji (przypadkowe)
5. Utrata dostaw prądu (przypadkowe)
6. Zmiana informacji (przypadkowe)
7. Ujawnienie (przypadkowe)
8. Sfałszowanie oprogramowania (przypadkowe)
9. Awaria urządzenia (przypadkowe)
10. Niewłaściwe funkcjonowanie oprogramowania (przypadkowe)
11. Awaria łączności (przypadkowe)
12. Błąd użytkowania (przypadkowy)
13. Błąd administrowania (przypadkowe)
14. Błąd monitorowania (przypadkowe)
15. Błąd konfiguracyjny (przypadkowe)
16. Naruszenie dostępności personelu (przypadkowe)
17. Naruszenie praw (przypadkowe)
18. Braki organizacyjne (przypadkowe)
19. Nieprawidłowa konserwacja sprzętu (przypadkowe)
20. Nieprawidłowa konserwacja oprogramowania (przypadkowe)

Zagrożenia umyślne
21. Pożar (umyślne)
22. Zniszczenie nośników (umyślne)
23. Zniszczenie urządzeń (umyślne)
24. Utrata dostaw prądu (umyślne)
25. Przerwy w łączności, transmisji danych (umyślne)
26. Awaria systemu klimatyzacji (umyślne)
27. Manipulacja konfiguracją (umyślne)
28. Podsłuch sieci LAN, WAN (umyślne)
29. Zmiana informacji (umyślne)
30. Skasowanie informacji (umyślne)
31. Ujawnienie (umyślne)
32. Kradzież nośników (umyślne)
33. Kradzież dokumentów (umyślne)
34. Kradzież urządzenia (umyślne)
35. Manipulacja urządzeniem (umyślne)
36. Sfałszowanie oprogramowania (umyślne)
37. Nieautoryzowany dostęp (umyślne)
38. Wtargnięcie (umyślne)
39. Socjotechnika (umyślne)
40. Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)
41. Złośliwe oprogramowanie (umyślne)

42. Naruszenie praw (umyślne)
43. Szpiegostwo zdalne (umyślne)

5. Lista podatności

W ramach identyfikacji ryzyka określono podatności zasobów. Przy czym podatność należy rozumieć jako słabość zasobu lub zabezpieczenia, która może zostać wykorzystana przez zagrożenie.

Sprzęt/Media
1. Niewłaściwa konserwacja sprzętu
2. Brak przeglądów okresowych
3. Wrażliwość na wilgoć, pył, zanieczyszczenie
4. Brak kontroli zmian konfiguracji sprzętu
5. Wrażliwość na zmiany napięcia zasilania
6. Wrażliwość na zmiany temperatury
7. Niekontrolowane kopiowanie
8. Brak zabezpieczenia plombami
9. Niewłaściwa lokalizacja sprzętu
10. Niewłaściwe oznaczenie nośników
11. Niepoprawne użycie oprogramowania lub sprzętu
12. Nieodpowiedni serwis sprzętu
13. Niewystarczające utrzymanie/błędna instalacja nośników pamięci
14. Brak skutecznej kontroli zmian konfiguracji
15. Niezabezpieczone urządzenia do przechowywania danych
16. Brak staranności przy pozbywaniu się nośników

Oprogramowanie
17. Dobrze znane wady oprogramowania
18. Brak wylogowania przy opuszczaniu stacji roboczej
19. Pozbywanie się lub ponowne używanie nośników bez właściwego wykasowania informacji
20. Brak śladu audytowego
21. Błędne przypisanie praw dostępu
22. Brak dokumentacji
23. Nieprawidłowa konfiguracja oprogramowania
24. Brak mechanizmów identyfikacji i uwierzyteleniania, takich jak uwierzytelnianie użytkownika
25. Niezabezpieczone tablice haseł
26. Złe zarządzanie hasłami
27. Uruchomione zbędne usługi
28. Niekontrolowane ściąganie i użytkowanie oprogramowania
29. Brak kopii zapasowych
30. Brak dostępnych aktualizacji oprogramowania
31. Brak wsparcia oprogramowania przez producenta
32. Brak lub niewłaściwa konfiguracja polityki bezpieczeństwa GPO
33. Niewłaściwa konfiguracja systemu operacyjnego i/lub oprogramowania
34. Brak aktualizacji systemu operacyjnego
35. Brak blokady domyślnych kont
36. Brak zmiany domyślnych haseł
37. Niewłaściwe przechowywanie danych elektronicznych
38. Nieprawidłowa konfiguracja
39. Brak lub nieaktualne sterowniki urządzeń
40. Nieprawidłowe daty

Sieć

41. Niechroniony wrażliwy ruch
42. Pojedynczy punkt uszkodzenia
43. Brak identyfikacji i uwierzytelnienia nadawcy i odbiorcy
44. Niezabezpieczona architektura sieciowa
45. Przesyłanie haseł w jawnej postaci
46. Niezabezpieczone połączenia z siecią publiczną

Personel
47. Nieobecność personelu
48. Niewystarczające szkolenie z bezpieczeństwa
49. Brak świadomości w zakresie bezpieczeństwa
50. Brak mechanizmów monitorowania
51. Praca personelu zewnętrznego lub sprzątającego bez nadzoru
52. Niekompetentny personel administrujący systemem teleinformatycznym
53. Niekompetentny personel kontrolujący
54. Brak polityki w zakresie poprawnego użytkowania środków telekomunikacyjnych i komunikatorów

Siedziba
55. Niechronione miejsca przechowywania danych na nośnikach lub w postaci dokumentów papierowych
56. Brak fizycznej ochrony budynków, drzwi i okien
57. Niestabilna sieć elektryczna
58. Ogólny dostęp do budynku dla osób trzecich
59. Brak personelu ochronnego
60. Brak systemu monitoringu wizyjnego CCTV
61. Brak systemu sygnalizacji włamania i napadu
62. Brak systemu przeciwpożarowego

Organizacja
63. Brak tworzenia raportów dla kierownictwa
64. Brak procedur właściwego użytkowania komputera
65. Brak prowadzenia regularnego audytu bezpieczeństwa systemu
66. Brak zapisów w dziennikach administatorów i operatorów
67. Brak ustanowionych mechanizmów monitorowania naruszeń bezpieczeństwa
68. Brak procedur bezpieczeństwa dla użytkownika
69. Brak procedur bezpieczeństwa dla inspektora ochrony danych osobowych
70. Brak procedur bezpieczeństwa dla administratora systemu
71. Brak zarządzania ryzykiem
72. Brak testów bezpieczeństwa
73. Brak szkoleń z zakresu bezpieczeństwa informacji i postępowania z dokumentami
74. Brak szkoleń z zakresu użytkowania systemu teleinformatycznego
75. Brak lub nieodpowiednia szafa do przechowywania
76. Nieprawidłowe zarządzanie hasłami w tym brak konfiguracji
77. Brak monitorowania dostępnych aktualizacji
78. Brak aktualizacji polityki bezpieczeństwa
79. Brak formalnej procedury rejestrowania i wyrejestrowywania użytkownika
80. Brak lub niewystarczające zapisy (odnoszące się do bezpieczeństwa) w umowie z klientami i/lub stronami trzecimi
81. Brak raportowania błędów rejestrowanych w dziennikach administratorów i operatorów
82. Nieodpowiednia reakcja utrzymania serwisowego
83. Brak formalnego procesu autoryzacji dla informacji publicznie dostępnych
84. Brak właściwego przypisania zakresów odpowiedzialności związanych z bezpieczeństwem informacji
85. Brak planów ciągłości
86. Brak polityki korzystania z poczty elektronicznej
87. Brak procedur instalacji oprogramowania w systemach produkcyjnych

88. Brak lub niewystarczające zapisy (odnoszące się do bezpieczeństwa informacji) w umowach z pracownikami
89. Brak formalnej polityki korzystania z komputerów przenośnych
90. Brak nadzoru nad aktywami znajdującymi się poza siedzibą
91. Brak lub niewystarczająca polityka czystego biurka i czystego ekranu
92. Brak procedur raportowania o słabościach bezpieczeństwa

6. Skala skutków i prawdopodobieństw

SKUTKI
Skutki ustalono dla każdego atrybutu informacji: poufności, dostępności i integralności. Przyjęto 10-stopniową wartość skali. Im większa wartość tym większy skutek działania zagrożenia na zasób.

Skutek utraty poufności / zachowanie poufności

Wartość	Poziom
0	Brak
1-2	Niskie
3-5	Średnie
6-8	Wysokie
9-10	Maksymalne

Skutek utraty integralności / zachowanie integralności

Wartość	Poziom
0	Brak
1-2	Niskie
3-5	Średnie
6-8	Wysokie
9-10	Maksymalne

Skutek utraty dostępności / Zachowanie dostępności

Wartość	Poziom
0	Brak
1-2	Niskie
3-5	Średnie
6-8	Wysokie
9-10	Maksymalne

PRAWDOPODOBIEŃSTWA
Prawdopodobieństwa przyjmują wartości od 0 do 1. Im większa wartość tym większe prawdopodobieństwo wystąpienia zagrożenia.

Podatność systemu

Wartość	Poziom
0	Brak
0,1 - 0,2	Bardzo niskie
0,3 - 0,4	Niskie

0,5 - 0,6	Średnie
0,7 - 0,8	Wysokie
0,9 - 1	Bardzo wysokie

7. Skala ryzyka

Ryzyko wyliczono ze wzoru: Ryzyko = Skutek * Prawdopodobieństwo. W związku z tym, że skala skutków jest 10-stopniowa, skala prawdopodobieństwa jest ułamkowa od 0-1 to skala ryzyka po wymnożeniu skutków i prawdopodobieństwa jest 10-stopniowa. Przyjęto następujące poziomy ryzyka dla obliczonych wartości liczbowych ryzyka.

(R)yzyko = (P)rawdopodobieństwo * (S)kutek

Ryzyko utraty poufności, dostępności i integralności

Poziomy ryzyk	
Wartość ryzyka	**Poziom ryzyka**
0	Brak
1-2	Niskie
3-5	Średnie
6-8	Wysokie
9-10	Maksymalne

8. Ryzyko akceptowalne

Przyjęto następującą wartość ryzyka akceptowalnego. Jest to poziom akceptowalny, powyżej którego należy zmniejszyć ryzyko.

Ryzyko akceptowalne: 4 (Średnie)

9. Lista zabezpieczeń

W w ramach identyfikacji ryzyka wdrożono poniższe zabezpieczenia. Zabezpieczenie jest to środek o charakterze fizycznym, technicznym lub organizacyjnym zmniejszający ryzyko. Poprzez wdrożenie poniższego zbioru zabezpieczeń zapewniono bezpieczeństwo danych osobowych.

Ogólne i narzędzia
1. Elektroniczne monitorowanie zdarzeń (logi)
2. Oprogramowanie antywirusowe
3. Logiczna kontrola dostępu
4. Minimalizacja funkcjonalności
5. Identyfikacja i uwierzytelnienie użytkownika
6. Hasła (złożone)
7. Blokada konta po bezczynności
8. Przechowywanie haseł administratora
9. Indywidualne konta w systemie TI

Ochrona informacji/danych
10. Kopia zapasowa
11. Zabezpieczenie monitora przed podglądem
12. Niszczarka dokumentów

Bezpieczeństwo osobowe / Personel
13. Szkolenia z obsługi oprogramowania dla użytkowników
14. Szkolenia z bezpieczeństwa dla użytkowników
15. Szkolenia dla administratorów
16. Nadzór (nad serwisantami)
17. Odpowiedzialność użytkowników

Ochrona oprogramowania
18. Regularna konserwacja i inwentaryzacja oprogramowania
19. Regularne aktualizacje systemu
20. Bezpieczna konfiguracja oprogramowania

Ochrona sprzętu
21. Sprzęt z certyfikatem CE
22. Regularna konserwacja i inwentaryzacja sprzętu
23. Serwis sprzętu komputerowego
24. Aktualizacja sterowników urządzeń

Ochrona nośników danych
25. Konserwacja i inwentaryzacja nośników
26. Bezpieczne przechowywanie nośników

Bezpieczeństwo fizyczne i środowiskowe
27. System wentylacji
28. Bezpieczne drzwi
29. Ochrona kluczy do pomieszczeń (obszarów)
30. Gaśnice

Organizacja
31. Plany awaryjne
32. Zarządzanie ryzykiem
33. Bieżąca kontrola
34. Bezpieczny hosting danych

Procedury i polityki bezpieczeństwa
35. Procedura zarządzania zmianami sprzętu
36. Procedury zarządzania incydentami bezpieczeństwa
37. Procedura wykonywania i odtworzenia kopii danych
38. Procedura użytkowania nośników elektronicznych
39. Procedura usuwania danych i niszczenia nośników elektronicznych
40. Procedura użytkowania stanowiska komputerowego
41. Procedura użytkowania urządzeń systemu
42. Polityka bezpieczeństwa
43. Procedury bezpieczeństwa

10. Macierz ryzyka po wdrożeniu zabezpieczeń

Po zastosowaniu zabezpieczeń nastąpiło obniżenie ryzyk naruszenia bezpieczeństwa. Ryzyka pozostające po procesie postępowania z ryzykiem (ryzyka szczątkowe) podlegają procesowi akceptacji ryzyka.

POUFNOŚĆ

POUFNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Dane osobowe na dysku twardym	Błąd użytkowania (przypadkowy)	0.1	1.1	0.1	TAK
Dane osobowe na dysku twardym	Błąd administrowania (przypadkowe)	0.2	2.3	0.5	TAK
Dane osobowe na dysku twardym	Błąd monitorowania (przypadkowe)	0.3	1.9	0.6	TAK
Dane osobowe na dysku twardym	Złośliwe oprogramowanie (umyślne)	0.3	5.5	1.7	TAK
Dane osobowe na dysku twardym	Ujawnienie (przypadkowe)	0.2	4.6	0.9	TAK
Dane osobowe na dysku twardym	Naruszenie praw (umyślne)	0.2	4.6	0.9	TAK
Dane osobowe na dysku twardym	Nieautoryzowany dostęp (umyślne)	0.2	6.0	1.2	TAK
Dane osobowe na dysku twardym	Ujawnienie (umyślne)	0.3	6.1	1.8	TAK
Dane osobowe na dysku twardym	Kradzież nośników (umyślne)	0.3	6.8	2.0	TAK
Dane osobowe na dysku twardym	Naruszenie praw (przypadkowe)	0.2	3.3	0.7	TAK
Dane osobowe na dysku twardym	Szpiegostwo zdalne (umyślne)	0.2	4.6	0.9	TAK
Dane osobowe na dysku twardym	Sfałszowanie oprogramowania (przypadkowe)	0.2	1.2	0.2	TAK
Dane osobowe na dysku twardym	Sfałszowanie oprogramowania (umyślne)	0.2	4.8	1.0	TAK
Dane osobowe na dysku twardym	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.2	5.7	1.1	TAK
Komputer PC	Błąd użytkowania (przypadkowy)	0.1	1.1	0.1	TAK
Komputer PC	Błąd administrowania (przypadkowe)	0.2	3.0	0.6	TAK
Komputer PC	Błąd monitorowania (przypadkowe)	0.3	1.8	0.5	TAK
Komputer PC	Złośliwe oprogramowanie (umyślne)	0.3	5.7	1.7	TAK
Komputer PC	Ujawnienie (przypadkowe)	0.2	4.2	0.8	TAK
Komputer PC	Manipulacja konfiguracją (umyślne)	0.2	4.5	0.9	TAK
Komputer PC	Naruszenie praw (umyślne)	0.2	4.2	0.8	TAK
Komputer PC	Nieautoryzowany dostęp (umyślne)	0.2	4.5	0.9	TAK
Komputer PC	Ujawnienie (umyślne)	0.3	5.0	1.5	TAK
Komputer PC	Kradzież nośników (umyślne)	0.3	6.7	2.0	TAK
Komputer PC	Naruszenie praw (przypadkowe)	0.2	3.1	0.6	TAK
Komputer PC	Szpiegostwo zdalne (umyślne)	0.2	6.0	1.2	TAK
Komputer PC	Kradzież urządzenia (umyślne)	0.4	3.8	1.5	TAK
Komputer PC	Sfałszowanie oprogramowania (przypadkowe)	0.2	1.1	0.2	TAK
Komputer PC	Sfałszowanie oprogramowania (umyślne)	0.2	4.6	0.9	TAK
Komputer PC	Użycie nielegalnego lub skopiowanego	0.3	5.4	1.6	TAK

POUFNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
	oprogramowania (umyślne)				
Drukarka	Błąd użytkowania (przypadkowy)	0.2	1.1	0.2	TAK
Drukarka	Błąd administrowania (przypadkowe)	0.3	3.0	0.9	TAK
Drukarka	Błąd monitorowania (przypadkowe)	0.4	1.8	0.7	TAK
Drukarka	Ujawnienie (przypadkowe)	0.2	3.6	0.7	TAK
Drukarka	Manipulacja konfiguracją (umyślne)	0.3	4.6	1.4	TAK
Drukarka	Naruszenie praw (umyślne)	0.3	3.6	1.1	TAK
Drukarka	Nieautoryzowany dostęp (umyślne)	0.3	4.8	1.4	TAK
Drukarka	Ujawnienie (umyślne)	0.3	4.5	1.3	TAK
Drukarka	Naruszenie praw (przypadkowe)	0.2	2.5	0.5	TAK
Drukarka	Szpiegostwo zdalne (umyślne)	0.4	3.0	1.2	TAK
Drukarka	Kradzież urządzenia (umyślne)	0.2	1.6	0.3	TAK
Drukarka	Sfałszowanie oprogramowania (przypadkowe)	0.4	1.3	0.5	TAK
Drukarka	Sfałszowanie oprogramowania (umyślne)	0.5	3.2	1.6	TAK
Drukarka	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.6	3.8	2.3	TAK
Dysk twardy	Ujawnienie (przypadkowe)	0.3	5.5	1.7	TAK
Dysk twardy	Nieautoryzowany dostęp (umyślne)	0.5	6.7	3.4	TAK
Dysk twardy	Ujawnienie (umyślne)	0.3	6.4	1.9	TAK
Dysk twardy	Kradzież nośników (umyślne)	0.3	6.8	2.0	TAK
Wydruki papierowe	Błąd użytkowania (przypadkowy)	0.3	1.3	0.4	TAK
Wydruki papierowe	Błąd administrowania (przypadkowe)	0.4	0.7	0.3	TAK
Wydruki papierowe	Ujawnienie (przypadkowe)	0.5	5.3	2.7	TAK
Wydruki papierowe	Nieautoryzowany dostęp (umyślne)	0.5	6.4	3.2	TAK
Wydruki papierowe	Ujawnienie (umyślne)	0.3	6.2	1.9	TAK
Wydruki papierowe	Kradzież dokumentów (umyślne)	0.3	6.3	1.9	TAK
Windows	Błąd użytkowania (przypadkowy)	0.1	1.1	0.1	TAK
Windows	Błąd administrowania (przypadkowe)	0.3	3.9	1.2	TAK
Windows	Błąd monitorowania (przypadkowe)	0.3	1.8	0.5	TAK
Windows	Złośliwe oprogramowanie (umyślne)	0.3	5.4	1.6	TAK
Windows	Ujawnienie (przypadkowe)	0.2	3.6	0.7	TAK
Windows	Manipulacja konfiguracją (umyślne)	0.3	4.8	1.4	TAK
Windows	Naruszenie praw (umyślne)	0.2	4.2	0.8	TAK
Windows	Nieautoryzowany dostęp (umyślne)	0.2	5.2	1.0	TAK
Windows	Ujawnienie (umyślne)	0.2	4.7	0.9	TAK
Windows	Naruszenie praw (przypadkowe)	0.2	3.1	0.6	TAK
Windows	Sfałszowanie oprogramowania (przypadkowe)	0.2	1.1	0.2	TAK
Windows	Sfałszowanie oprogramowania (umyślne)	0.2	4.6	0.9	TAK
Windows	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.3	5.4	1.6	TAK
Pakiet biurowy office	Błąd użytkowania (przypadkowy)	0.2	2.3	0.5	TAK
Pakiet biurowy office	Błąd administrowania (przypadkowe)	0.2	3.0	0.6	TAK
Pakiet biurowy office	Błąd monitorowania (przypadkowe)	0.3	1.8	0.5	TAK
Pakiet biurowy office	Złośliwe oprogramowanie (umyślne)	0.3	5.7	1.7	TAK
Pakiet biurowy office	Ujawnienie (przypadkowe)	0.2	3.6	0.7	TAK
Pakiet biurowy office	Manipulacja konfiguracją (umyślne)	0.3	4.8	1.4	TAK
Pakiet biurowy office	Naruszenie praw (umyślne)	0.2	4.2	0.8	TAK
Pakiet biurowy office	Nieautoryzowany dostęp (umyślne)	0.2	4.6	0.9	TAK
Pakiet biurowy office	Ujawnienie (umyślne)	0.3	5.3	1.6	TAK
Pakiet biurowy office	Naruszenie praw (przypadkowe)	0.2	3.1	0.6	TAK
Pakiet biurowy office	Szpiegostwo zdalne (umyślne)	0.2	5.4	1.1	TAK
Pakiet biurowy office	Sfałszowanie oprogramowania	0.2	1.1	0.2	TAK

POUFNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
	(przypadkowe)				
Pakiet biurowy office	Sfałszowanie oprogramowania (umyślne)	0.2	4.6	0.9	TAK
Pakiet biurowy office	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.2	5.4	1.1	TAK
Oprogramowanie do zarządzania klientami	Błąd użytkowania (przypadkowy)	0.1	1.1	0.1	TAK
Oprogramowanie do zarządzania klientami	Błąd administrowania (przypadkowe)	0.2	3.0	0.6	TAK
Oprogramowanie do zarządzania klientami	Błąd monitorowania (przypadkowe)	0.3	1.8	0.5	TAK
Oprogramowanie do zarządzania klientami	Złośliwe oprogramowanie (umyślne)	0.3	5.7	1.7	TAK
Oprogramowanie do zarządzania klientami	Ujawnienie (przypadkowe)	0.2	3.6	0.7	TAK
Oprogramowanie do zarządzania klientami	Manipulacja konfiguracją (umyślne)	0.3	4.8	1.4	TAK
Oprogramowanie do zarządzania klientami	Naruszenie praw (umyślne)	0.2	4.2	0.8	TAK
Oprogramowanie do zarządzania klientami	Nieautoryzowany dostęp (umyślne)	0.2	5.2	1.0	TAK
Oprogramowanie do zarządzania klientami	Ujawnienie (umyślne)	0.3	5.3	1.6	TAK
Oprogramowanie do zarządzania klientami	Naruszenie praw (przypadkowe)	0.2	3.1	0.6	TAK
Oprogramowanie do zarządzania klientami	Szpiegostwo zdalne (umyślne)	0.2	5.4	1.1	TAK
Oprogramowanie do zarządzania klientami	Sfałszowanie oprogramowania (przypadkowe)	0.2	1.1	0.2	TAK
Oprogramowanie do zarządzania klientami	Sfałszowanie oprogramowania (umyślne)	0.2	4.6	0.9	TAK
Oprogramowanie do zarządzania klientami	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.2	5.4	1.1	TAK
Użytkownik	Ujawnienie (przypadkowe)	0.3	4.1	1.2	TAK
Użytkownik	Ujawnienie (umyślne)	0.5	5.9	3.0	TAK
Użytkownik	Socjotechnika (umyślne)	0.3	4.7	1.4	TAK
Administrator systemu	Ujawnienie (przypadkowe)	0.4	4.1	1.6	TAK
Administrator systemu	Ujawnienie (umyślne)	0.5	6.6	3.3	TAK
Administrator systemu	Socjotechnika (umyślne)	0.4	5.5	2.2	TAK
Pomieszczenie	Nieautoryzowany dostęp (umyślne)	0.5	5.8	2.9	TAK
Pomieszczenie	Wtargnięcie (umyślne)	0.4	3.4	1.4	TAK

DOSTĘPNOŚĆ

DOSTĘPNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Dane osobowe na dysku twardym	Pożar (umyślne)	0.5	4.3	2.2	TAK
Dane osobowe na dysku twardym	Pożar (naturalne)	0.2	4.5	0.9	TAK
Dane osobowe na dysku twardym	Awaria urządzenia (przypadkowe)	0.2	6.0	1.2	TAK
Dane osobowe na dysku twardym	Niewłaściwe funkcjonowanie oprogramowania (przypadkowe)	0.2	5.0	1.0	TAK

DOSTĘPNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Dane osobowe na dysku twardym	Błąd użytkowania (przypadkowy)	0.1	3.3	0.3	TAK
Dane osobowe na dysku twardym	Błąd administrowania (przypadkowe)	0.2	6.6	1.3	TAK
Dane osobowe na dysku twardym	Błąd monitorowania (przypadkowe)	0.3	5.5	1.7	TAK
Dane osobowe na dysku twardym	Złośliwe oprogramowanie (umyślne)	0.3	7.8	2.3	TAK
Dane osobowe na dysku twardym	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.2	7.0	1.4	TAK
Dane osobowe na dysku twardym	Nieautoryzowany dostęp (umyślne)	0.2	4.3	0.9	TAK
Dane osobowe na dysku twardym	Skasowanie informacji (umyślne)	0.3	7.8	2.3	TAK
Dane osobowe na dysku twardym	Kradzież nośników (umyślne)	0.3	9.7	2.9	TAK
Dane osobowe na dysku twardym	Zniszczenie nośników (umyślne)	0.3	7.9	2.4	TAK
Dane osobowe na dysku twardym	Pożar (przypadkowe)	0.3	6.0	1.8	TAK
Dane osobowe na dysku twardym	Zniszczenie urządzeń (umyślne)	0.4	8.7	3.5	TAK
Dane osobowe na dysku twardym	Manipulacja urządzeniem (umyślne)	0.4	6.9	2.8	TAK
Dane osobowe na dysku twardym	Sfałszowanie oprogramowania (przypadkowe)	0.2	5.2	1.0	TAK
Dane osobowe na dysku twardym	Sfałszowanie oprogramowania (umyślne)	0.2	6.9	1.4	TAK
Dane osobowe na dysku twardym	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.2	6.4	1.3	TAK
Komputer PC	Pożar (umyślne)	0.4	6.8	2.7	TAK
Komputer PC	Pożar (naturalne)	0.2	7.0	1.4	TAK
Komputer PC	Awaria urządzenia (przypadkowe)	0.3	5.4	1.6	TAK
Komputer PC	Niewłaściwe funkcjonowanie oprogramowania (przypadkowe)	0.2	5.0	1.0	TAK
Komputer PC	Utrata dostaw prądu (naturalne)	0.2	10.0	2.0	TAK
Komputer PC	Awaria łączności (przypadkowe)	0.1	3.0	0.3	TAK
Komputer PC	Błąd użytkowania (przypadkowy)	0.1	3.3	0.3	TAK
Komputer PC	Błąd administrowania (przypadkowe)	0.2	6.0	1.2	TAK
Komputer PC	Błąd monitorowania (przypadkowe)	0.3	5.2	1.6	TAK
Komputer PC	Błąd konfiguracyjny (przypadkowe)	0.3	5.3	1.6	TAK
Komputer PC	Złośliwe oprogramowanie (umyślne)	0.3	8.1	2.4	TAK
Komputer PC	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.3	6.1	1.8	TAK
Komputer PC	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.3	3.4	1.0	TAK
Komputer PC	Manipulacja konfiguracją (umyślne)	0.2	6.4	1.3	TAK
Komputer PC	Nieautoryzowany dostęp (umyślne)	0.2	4.8	1.0	TAK
Komputer PC	Skasowanie informacji (umyślne)	0.3	9.8	2.9	TAK
Komputer PC	Kradzież nośników (umyślne)	0.3	9.5	2.9	TAK
Komputer PC	Utrata dostaw prądu (przypadkowe)	0.1	8.5	0.9	TAK
Komputer PC	Utrata dostaw prądu (umyślne)	0.4	8.8	3.5	TAK
Komputer PC	Zniszczenie nośników (umyślne)	0.3	9.4	2.8	TAK
Komputer PC	Przerwy w łączności, transmisji danych (umyślne)	0.4	2.7	1.1	TAK
Komputer PC	Pożar (przypadkowe)	0.3	6.8	2.0	TAK
Komputer PC	Zniszczenie urządzeń (umyślne)	0.3	7.7	2.3	TAK

DOSTĘPNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Komputer PC	Kradzież urządzenia (umyślne)	0.4	7.8	3.1	TAK
Komputer PC	Manipulacja urządzeniem (umyślne)	0.4	6.2	2.5	TAK
Komputer PC	Sfałszowanie oprogramowania (przypadkowe)	0.2	4.9	1.0	TAK
Komputer PC	Sfałszowanie oprogramowania (umyślne)	0.2	6.6	1.3	TAK
Komputer PC	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.3	6.0	1.8	TAK
Drukarka	Pożar (umyślne)	0.4	6.8	2.7	TAK
Drukarka	Pożar (naturalne)	0.2	7.0	1.4	TAK
Drukarka	Awaria urządzenia (przypadkowe)	0.3	6.0	1.8	TAK
Drukarka	Niewłaściwe funkcjonowanie oprogramowania (przypadkowe)	0.3	5.0	1.5	TAK
Drukarka	Utrata dostaw prądu (naturalne)	0.3	10.0	3.0	TAK
Drukarka	Awaria łączności (przypadkowe)	0.2	3.0	0.6	TAK
Drukarka	Błąd użytkowania (przypadkowy)	0.2	3.3	0.7	TAK
Drukarka	Błąd administrowania (przypadkowe)	0.3	6.0	1.8	TAK
Drukarka	Błąd monitorowania (przypadkowe)	0.4	5.2	2.1	TAK
Drukarka	Błąd konfiguracyjny (przypadkowe)	0.4	5.4	2.2	TAK
Drukarka	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.3	6.5	2.0	TAK
Drukarka	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.5	3.5	1.8	TAK
Drukarka	Manipulacja konfiguracją (umyślne)	0.3	6.6	2.0	TAK
Drukarka	Nieautoryzowany dostęp (umyślne)	0.3	4.3	1.3	TAK
Drukarka	Skasowanie informacji (umyślne)	0.2	4.9	1.0	TAK
Drukarka	Utrata dostaw prądu (przypadkowe)	0.2	8.7	1.7	TAK
Drukarka	Utrata dostaw prądu (umyślne)	0.4	8.8	3.5	TAK
Drukarka	Przerwy w łączności, transmisji danych (umyślne)	0.5	4.6	2.3	TAK
Drukarka	Pożar (przypadkowe)	0.3	6.8	2.0	TAK
Drukarka	Zniszczenie urządzeń (umyślne)	0.3	8.2	2.5	TAK
Drukarka	Kradzież urządzenia (umyślne)	0.2	6.2	1.2	TAK
Drukarka	Manipulacja urządzeniem (umyślne)	0.4	6.6	2.6	TAK
Drukarka	Sfałszowanie oprogramowania (przypadkowe)	0.4	5.5	2.2	TAK
Drukarka	Sfałszowanie oprogramowania (umyślne)	0.5	7.4	3.7	TAK
Drukarka	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.6	6.3	3.8	TAK
Dysk twardy	Pożar (umyślne)	0.5	6.8	3.4	TAK
Dysk twardy	Pożar (naturalne)	0.2	7.0	1.4	TAK
Dysk twardy	Awaria urządzenia (przypadkowe)	0.2	6.0	1.2	TAK
Dysk twardy	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.2	7.4	1.5	TAK
Dysk twardy	Nieautoryzowany dostęp (umyślne)	0.5	4.8	2.4	TAK
Dysk twardy	Skasowanie informacji (umyślne)	0.4	10.0	4.0	TAK
Dysk twardy	Kradzież nośników (umyślne)	0.3	9.7	2.9	TAK
Dysk twardy	Zniszczenie nośników (umyślne)	0.3	9.4	2.8	TAK
Dysk twardy	Pożar (przypadkowe)	0.3	6.8	2.0	TAK
Dysk twardy	Zniszczenie urządzeń (umyślne)	0.4	9.1	3.6	TAK
Dysk twardy	Manipulacja urządzeniem (umyślne)	0.5	6.9	3.5	TAK
Wydruki papierowe	Pożar (umyślne)	0.5	6.8	3.4	TAK
Wydruki papierowe	Pożar (naturalne)	0.2	7.0	1.4	TAK
Wydruki papierowe	Błąd użytkowania (przypadkowy)	0.3	3.7	1.1	TAK
Wydruki papierowe	Błąd administrowania (przypadkowe)	0.4	6.5	2.6	TAK

DOSTĘPNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Wydruki papierowe	Nieautoryzowany dostęp (umyślne)	0.5	4.6	2.3	TAK
Wydruki papierowe	Pożar (przypadkowe)	0.3	6.8	2.0	TAK
Wydruki papierowe	Kradzież dokumentów (umyślne)	0.3	9.0	2.7	TAK
Windows	Niewłaściwe funkcjonowanie oprogramowania (przypadkowe)	0.2	5.0	1.0	TAK
Windows	Błąd użytkowania (przypadkowy)	0.1	3.1	0.3	TAK
Windows	Błąd administrowania (przypadkowe)	0.3	6.4	1.9	TAK
Windows	Błąd monitorowania (przypadkowe)	0.3	5.2	1.6	TAK
Windows	Błąd konfiguracyjny (przypadkowe)	0.4	5.1	2.0	TAK
Windows	Złośliwe oprogramowanie (umyślne)	0.3	7.7	2.3	TAK
Windows	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.4	3.4	1.4	TAK
Windows	Manipulacja konfiguracją (umyślne)	0.3	6.8	2.0	TAK
Windows	Nieautoryzowany dostęp (umyślne)	0.2	4.2	0.8	TAK
Windows	Skasowanie informacji (umyślne)	0.3	8.3	2.5	TAK
Windows	Sfałszowanie oprogramowania (przypadkowe)	0.2	4.9	1.0	TAK
Windows	Sfałszowanie oprogramowania (umyślne)	0.2	6.6	1.3	TAK
Windows	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.3	6.0	1.8	TAK
Pakiet biurowy office	Niewłaściwe funkcjonowanie oprogramowania (przypadkowe)	0.2	5.0	1.0	TAK
Pakiet biurowy office	Błąd użytkowania (przypadkowy)	0.2	3.3	0.7	TAK
Pakiet biurowy office	Błąd administrowania (przypadkowe)	0.2	6.8	1.4	TAK
Pakiet biurowy office	Błąd monitorowania (przypadkowe)	0.3	5.2	1.6	TAK
Pakiet biurowy office	Błąd konfiguracyjny (przypadkowe)	0.3	5.4	1.6	TAK
Pakiet biurowy office	Złośliwe oprogramowanie (umyślne)	0.3	8.1	2.4	TAK
Pakiet biurowy office	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.3	3.4	1.0	TAK
Pakiet biurowy office	Manipulacja konfiguracją (umyślne)	0.3	6.8	2.0	TAK
Pakiet biurowy office	Nieautoryzowany dostęp (umyślne)	0.2	4.2	0.8	TAK
Pakiet biurowy office	Skasowanie informacji (umyślne)	0.3	8.8	2.6	TAK
Pakiet biurowy office	Sfałszowanie oprogramowania (przypadkowe)	0.2	4.9	1.0	TAK
Pakiet biurowy office	Sfałszowanie oprogramowania (umyślne)	0.2	6.6	1.3	TAK
Pakiet biurowy office	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.2	6.0	1.2	TAK
Oprogramowanie do zarządzania klientami	Niewłaściwe funkcjonowanie oprogramowania (przypadkowe)	0.2	5.0	1.0	TAK
Oprogramowanie do zarządzania klientami	Błąd użytkowania (przypadkowy)	0.1	3.3	0.3	TAK
Oprogramowanie do zarządzania klientami	Błąd administrowania (przypadkowe)	0.2	6.8	1.4	TAK
Oprogramowanie do zarządzania klientami	Błąd monitorowania (przypadkowe)	0.3	5.2	1.6	TAK
Oprogramowanie do zarządzania klientami	Błąd konfiguracyjny (przypadkowe)	0.3	5.4	1.6	TAK
Oprogramowanie do zarządzania klientami	Złośliwe oprogramowanie (umyślne)	0.3	8.1	2.4	TAK
Oprogramowanie do zarządzania klientami	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.3	3.4	1.0	TAK
Oprogramowanie do zarządzania klientami	Manipulacja konfiguracją (umyślne)	0.3	6.8	2.0	TAK
Oprogramowanie do zarządzania klientami	Nieautoryzowany dostęp (umyślne)	0.2	4.2	0.8	TAK

DOSTĘPNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Oprogramowanie do zarządzania klientami	Skasowanie informacji (umyślne)	0.2	7.8	1.6	TAK
Oprogramowanie do zarządzania klientami	Sfałszowanie oprogramowania (przypadkowe)	0.2	4.9	1.0	TAK
Oprogramowanie do zarządzania klientami	Sfałszowanie oprogramowania (umyślne)	0.2	6.6	1.3	TAK
Oprogramowanie do zarządzania klientami	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.2	6.0	1.2	TAK
Użytkownik	Braki organizacyjne (przypadkowe)	0.3	3.5	1.1	TAK
Użytkownik	Naruszenie dostępności personelu (przypadkowe)	0.1	4.3	0.4	TAK
Użytkownik	Socjotechnika (umyślne)	0.3	2.9	0.9	TAK
Administrator systemu	Braki organizacyjne (przypadkowe)	0.5	6.2	3.1	TAK
Administrator systemu	Naruszenie dostępności personelu (przypadkowe)	0.1	4.3	0.4	TAK
Administrator systemu	Socjotechnika (umyślne)	0.4	3.9	1.6	TAK
Pomieszczenie	Pożar (umyślne)	0.4	6.8	2.7	TAK
Pomieszczenie	Pożar (naturalne)	0.2	7.0	1.4	TAK
Pomieszczenie	Nieautoryzowany dostęp (umyślne)	0.5	4.6	2.3	TAK
Pomieszczenie	Wtargnięcie (umyślne)	0.4	8.6	3.4	TAK
Pomieszczenie	Pożar (przypadkowe)	0.3	6.8	2.0	TAK

INTEGRALNOŚĆ

INTEGRALNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Dane osobowe na dysku twardym	Błąd użytkowania (przypadkowy)	0.1	4.9	0.5	TAK
Dane osobowe na dysku twardym	Błąd administrowania (przypadkowe)	0.2	3.3	0.7	TAK
Dane osobowe na dysku twardym	Błąd monitorowania (przypadkowe)	0.3	4.6	1.4	TAK
Dane osobowe na dysku twardym	Złośliwe oprogramowanie (umyślne)	0.3	7.8	2.3	TAK
Dane osobowe na dysku twardym	Zmiana informacji (przypadkowe)	0.2	2.7	0.5	TAK
Dane osobowe na dysku twardym	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.2	2.6	0.5	TAK
Dane osobowe na dysku twardym	Nieautoryzowany dostęp (umyślne)	0.2	1.7	0.3	TAK
Dane osobowe na dysku twardym	Zmiana informacji (umyślne)	0.3	8.5	2.6	TAK
Dane osobowe na dysku twardym	Sfałszowanie oprogramowania (przypadkowe)	0.2	3.4	0.7	TAK
Dane osobowe na dysku twardym	Sfałszowanie oprogramowania (umyślne)	0.2	3.4	0.7	TAK
Dane osobowe na dysku twardym	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.2	4.6	0.9	TAK
Komputer PC	Błąd użytkowania (przypadkowy)	0.1	4.9	0.5	TAK
Komputer PC	Błąd administrowania (przypadkowe)	0.2	3.4	0.7	TAK
Komputer PC	Błąd monitorowania (przypadkowe)	0.3	4.4	1.3	TAK
Komputer PC	Błąd konfiguracyjny (przypadkowe)	0.3	1.5	0.5	TAK
Komputer PC	Złośliwe oprogramowanie (umyślne)	0.3	8.1	2.4	TAK
Komputer PC	Zmiana informacji (przypadkowe)	0.2	3.0	0.6	TAK

INTEGRALNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Komputer PC	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.3	2.3	0.7	TAK
Komputer PC	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.3	1.7	0.5	TAK
Komputer PC	Manipulacja konfiguracją (umyślne)	0.2	3.2	0.6	TAK
Komputer PC	Nieautoryzowany dostęp (umyślne)	0.2	4.0	0.8	TAK
Komputer PC	Zmiana informacji (umyślne)	0.2	8.3	1.7	TAK
Komputer PC	Sfałszowanie oprogramowania (przypadkowe)	0.2	3.3	0.7	TAK
Komputer PC	Sfałszowanie oprogramowania (umyślne)	0.2	3.3	0.7	TAK
Komputer PC	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.3	4.3	1.3	TAK
Drukarka	Błąd użytkowania (przypadkowy)	0.2	4.9	1.0	TAK
Drukarka	Błąd administrowania (przypadkowe)	0.3	3.4	1.0	TAK
Drukarka	Błąd monitorowania (przypadkowe)	0.4	4.4	1.8	TAK
Drukarka	Błąd konfiguracyjny (przypadkowe)	0.4	1.5	0.6	TAK
Drukarka	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.3	2.4	0.7	TAK
Drukarka	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.5	1.7	0.9	TAK
Drukarka	Manipulacja konfiguracją (umyślne)	0.3	1.6	0.5	TAK
Drukarka	Nieautoryzowany dostęp (umyślne)	0.3	3.4	1.0	TAK
Drukarka	Sfałszowanie oprogramowania (przypadkowe)	0.4	3.7	1.5	TAK
Drukarka	Sfałszowanie oprogramowania (umyślne)	0.5	3.7	1.9	TAK
Drukarka	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.6	4.5	2.7	TAK
Dysk twardy	Zmiana informacji (przypadkowe)	0.3	3.0	0.9	TAK
Dysk twardy	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.2	2.8	0.6	TAK
Dysk twardy	Nieautoryzowany dostęp (umyślne)	0.5	4.8	2.4	TAK
Dysk twardy	Zmiana informacji (umyślne)	0.5	7.0	3.5	TAK
Wydruki papierowe	Błąd użytkowania (przypadkowy)	0.3	5.5	1.7	TAK
Wydruki papierowe	Błąd administrowania (przypadkowe)	0.4	3.7	1.5	TAK
Wydruki papierowe	Nieautoryzowany dostęp (umyślne)	0.5	4.6	2.3	TAK
Windows	Błąd użytkowania (przypadkowy)	0.1	4.6	0.5	TAK
Windows	Błąd administrowania (przypadkowe)	0.3	3.2	1.0	TAK
Windows	Błąd monitorowania (przypadkowe)	0.3	4.4	1.3	TAK
Windows	Błąd konfiguracyjny (przypadkowe)	0.4	1.5	0.6	TAK
Windows	Złośliwe oprogramowanie (umyślne)	0.3	7.7	2.3	TAK
Windows	Zmiana informacji (przypadkowe)	0.2	2.9	0.6	TAK
Windows	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.4	1.7	0.7	TAK
Windows	Manipulacja konfiguracją (umyślne)	0.3	3.4	1.0	TAK
Windows	Nieautoryzowany dostęp (umyślne)	0.2	4.2	0.8	TAK
Windows	Zmiana informacji (umyślne)	0.3	7.8	2.3	TAK
Windows	Sfałszowanie oprogramowania (przypadkowe)	0.2	3.3	0.7	TAK
Windows	Sfałszowanie oprogramowania (umyślne)	0.2	3.3	0.7	TAK
Windows	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.3	4.3	1.3	TAK
Pakiet biurowy office	Błąd użytkowania (przypadkowy)	0.2	4.9	1.0	TAK
Pakiet biurowy office	Błąd administrowania (przypadkowe)	0.2	3.4	0.7	TAK

INTEGRALNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Pakiet biurowy office	Błąd monitorowania (przypadkowe)	0.3	4.4	1.3	TAK
Pakiet biurowy office	Błąd konfiguracyjny (przypadkowe)	0.3	1.5	0.5	TAK
Pakiet biurowy office	Złośliwe oprogramowanie (umyślne)	0.3	8.1	2.4	TAK
Pakiet biurowy office	Zmiana informacji (przypadkowe)	0.2	3.0	0.6	TAK
Pakiet biurowy office	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.3	1.7	0.5	TAK
Pakiet biurowy office	Manipulacja konfiguracją (umyślne)	0.3	3.4	1.0	TAK
Pakiet biurowy office	Nieautoryzowany dostęp (umyślne)	0.2	4.2	0.8	TAK
Pakiet biurowy office	Zmiana informacji (umyślne)	0.3	8.3	2.5	TAK
Pakiet biurowy office	Sfałszowanie oprogramowania (przypadkowe)	0.2	3.3	0.7	TAK
Pakiet biurowy office	Sfałszowanie oprogramowania (umyślne)	0.2	3.3	0.7	TAK
Pakiet biurowy office	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.2	4.3	0.9	TAK
Oprogramowanie do zarządzania klientami	Błąd użytkowania (przypadkowy)	0.1	4.9	0.5	TAK
Oprogramowanie do zarządzania klientami	Błąd administrowania (przypadkowe)	0.2	3.4	0.7	TAK
Oprogramowanie do zarządzania klientami	Błąd monitorowania (przypadkowe)	0.3	4.4	1.3	TAK
Oprogramowanie do zarządzania klientami	Błąd konfiguracyjny (przypadkowe)	0.3	1.5	0.5	TAK
Oprogramowanie do zarządzania klientami	Złośliwe oprogramowanie (umyślne)	0.3	8.1	2.4	TAK
Oprogramowanie do zarządzania klientami	Zmiana informacji (przypadkowe)	0.2	3.0	0.6	TAK
Oprogramowanie do zarządzania klientami	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.3	1.7	0.5	TAK
Oprogramowanie do zarządzania klientami	Manipulacja konfiguracją (umyślne)	0.3	3.4	1.0	TAK
Oprogramowanie do zarządzania klientami	Nieautoryzowany dostęp (umyślne)	0.2	4.2	0.8	TAK
Oprogramowanie do zarządzania klientami	Zmiana informacji (umyślne)	0.3	8.3	2.5	TAK
Oprogramowanie do zarządzania klientami	Sfałszowanie oprogramowania (przypadkowe)	0.2	3.3	0.7	TAK
Oprogramowanie do zarządzania klientami	Sfałszowanie oprogramowania (umyślne)	0.2	3.3	0.7	TAK
Oprogramowanie do zarządzania klientami	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.2	4.3	0.9	TAK
Użytkownik	Socjotechnika (umyślne)	0.3	1.0	0.3	TAK
Administrator systemu	Socjotechnika (umyślne)	0.4	1.0	0.4	TAK
Pomieszczenie	Nieautoryzowany dostęp (umyślne)	0.5	1.8	0.9	TAK

11. Ocena ryzyka

Na etapie oceny ryzyka określa się, które ryzyka są akceptowalne poprzez porównanie wyznaczonych poziomów ryzyk z ryzykiem, które można zaakceptować. W przypadku gdy ryzyka są większe od ryzyka akceptowalnego wprowadza się działania zaradcze (proces postępowania z ryzykiem). Dla ryzyk, które nie mogą być zaakceptowane ze względu na ich zbyt wysoki poziom, proces postępowania z ryzykiem przeprowadza się ponownie. Ryzyka pozostające po procesie postępowania z ryzykiem (ryzyka szczątkowe) podlegają procesowi akceptacji ryzyka.

Ryzyka naruszenia bezpieczeństwa zostały posortowane od największego do najmniejszego. Poniżej przedstawiono 100 największych wartości w tablie oceny ryzyka dla poufności, dostępności i integralności.

Ryzyko akceptowalne: 4

POUFNOŚĆ			
AKTYWA	**ZAGROŻENIA**	**RYZYKO**	**AKC**
Dysk twardy	Nieautoryzowany dostęp (umyślne)	3.4	TAK
Administrator systemu	Ujawnienie (umyślne)	3.3	TAK
Wydruki papierowe	Nieautoryzowany dostęp (umyślne)	3.2	TAK
Użytkownik	Ujawnienie (umyślne)	3.0	TAK
Pomieszczenie	Nieautoryzowany dostęp (umyślne)	2.9	TAK
Wydruki papierowe	Ujawnienie (przypadkowe)	2.7	TAK
Drukarka	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	2.3	TAK
Administrator systemu	Socjotechnika (umyślne)	2.2	TAK
Dane osobowe na dysku twardym	Kradzież nośników (umyślne)	2.0	TAK
Komputer PC	Kradzież nośników (umyślne)	2.0	TAK
Dysk twardy	Kradzież nośników (umyślne)	2.0	TAK
Dysk twardy	Ujawnienie (umyślne)	1.9	TAK
Wydruki papierowe	Ujawnienie (umyślne)	1.9	TAK
Wydruki papierowe	Kradzież dokumentów (umyślne)	1.9	TAK
Dane osobowe na dysku twardym	Ujawnienie (umyślne)	1.8	TAK
Dane osobowe na dysku twardym	Złośliwe oprogramowanie (umyślne)	1.7	TAK
Komputer PC	Złośliwe oprogramowanie (umyślne)	1.7	TAK
Dysk twardy	Ujawnienie (przypadkowe)	1.7	TAK
Pakiet biurowy office	Złośliwe oprogramowanie (umyślne)	1.7	TAK
Oprogramowanie do zarządzania klientami	Złośliwe oprogramowanie (umyślne)	1.7	TAK
Komputer PC	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.6	TAK
Drukarka	Sfałszowanie oprogramowania (umyślne)	1.6	TAK
Windows	Złośliwe oprogramowanie (umyślne)	1.6	TAK
Windows	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.6	TAK
Pakiet biurowy office	Ujawnienie (umyślne)	1.6	TAK
Oprogramowanie do zarządzania klientami	Ujawnienie (umyślne)	1.6	TAK
Administrator systemu	Ujawnienie (przypadkowe)	1.6	TAK
Komputer PC	Ujawnienie (umyślne)	1.5	TAK

POUFNOŚĆ			
AKTYWA	**ZAGROŻENIA**	**RYZYKO**	**AKC**
Komputer PC	Kradzież urządzenia (umyślne)	1.5	TAK
Drukarka	Manipulacja konfiguracją (umyślne)	1.4	TAK
Drukarka	Nieautoryzowany dostęp (umyślne)	1.4	TAK
Windows	Manipulacja konfiguracją (umyślne)	1.4	TAK
Pakiet biurowy office	Manipulacja konfiguracją (umyślne)	1.4	TAK
Oprogramowanie do zarządzania klientami	Manipulacja konfiguracją (umyślne)	1.4	TAK
Użytkownik	Socjotechnika (umyślne)	1.4	TAK
Pomieszczenie	Wtargnięcie (umyślne)	1.4	TAK
Drukarka	Ujawnienie (umyślne)	1.3	TAK
Dane osobowe na dysku twardym	Nieautoryzowany dostęp (umyślne)	1.2	TAK
Komputer PC	Szpiegostwo zdalne (umyślne)	1.2	TAK
Drukarka	Szpiegostwo zdalne (umyślne)	1.2	TAK
Windows	Błąd administrowania (przypadkowe)	1.2	TAK
Użytkownik	Ujawnienie (przypadkowe)	1.2	TAK
Dane osobowe na dysku twardym	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.1	TAK
Drukarka	Naruszenie praw (umyślne)	1.1	TAK
Pakiet biurowy office	Szpiegostwo zdalne (umyślne)	1.1	TAK
Pakiet biurowy office	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.1	TAK
Oprogramowanie do zarządzania klientami	Szpiegostwo zdalne (umyślne)	1.1	TAK
Oprogramowanie do zarządzania klientami	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.1	TAK
Dane osobowe na dysku twardym	Sfałszowanie oprogramowania (umyślne)	1.0	TAK
Windows	Nieautoryzowany dostęp (umyślne)	1.0	TAK
Oprogramowanie do zarządzania klientami	Nieautoryzowany dostęp (umyślne)	1.0	TAK
Dane osobowe na dysku twardym	Ujawnienie (przypadkowe)	0.9	TAK
Dane osobowe na dysku twardym	Naruszenie praw (umyślne)	0.9	TAK
Dane osobowe na dysku twardym	Szpiegostwo zdalne (umyślne)	0.9	TAK
Komputer PC	Manipulacja konfiguracją (umyślne)	0.9	TAK
Komputer PC	Nieautoryzowany dostęp (umyślne)	0.9	TAK
Komputer PC	Sfałszowanie oprogramowania (umyślne)	0.9	TAK
Drukarka	Błąd administrowania (przypadkowe)	0.9	TAK
Windows	Ujawnienie (umyślne)	0.9	TAK
Windows	Sfałszowanie oprogramowania (umyślne)	0.9	TAK
Pakiet biurowy office	Nieautoryzowany dostęp (umyślne)	0.9	TAK
Pakiet biurowy office	Sfałszowanie oprogramowania (umyślne)	0.9	TAK
Oprogramowanie do zarządzania klientami	Sfałszowanie oprogramowania (umyślne)	0.9	TAK
Komputer PC	Ujawnienie (przypadkowe)	0.8	TAK
Komputer PC	Naruszenie praw (umyślne)	0.8	TAK
Windows	Naruszenie praw (umyślne)	0.8	TAK
Pakiet biurowy office	Naruszenie praw (umyślne)	0.8	TAK
Oprogramowanie do zarządzania klientami	Naruszenie praw (umyślne)	0.8	TAK
Dane osobowe na dysku twardym	Naruszenie praw (przypadkowe)	0.7	TAK
Drukarka	Błąd monitorowania (przypadkowe)	0.7	TAK
Drukarka	Ujawnienie (przypadkowe)	0.7	TAK
Windows	Ujawnienie (przypadkowe)	0.7	TAK
Pakiet biurowy office	Ujawnienie (przypadkowe)	0.7	TAK
Oprogramowanie do zarządzania klientami	Ujawnienie (przypadkowe)	0.7	TAK
Dane osobowe na dysku twardym	Błąd monitorowania (przypadkowe)	0.6	TAK

POUFNOŚĆ			
AKTYWA	**ZAGROŻENIA**	**RYZYKO**	**AKC**
Komputer PC	Błąd administrowania (przypadkowe)	0.6	TAK
Komputer PC	Naruszenie praw (przypadkowe)	0.6	TAK
Windows	Naruszenie praw (przypadkowe)	0.6	TAK
Pakiet biurowy office	Błąd administrowania (przypadkowe)	0.6	TAK
Pakiet biurowy office	Naruszenie praw (przypadkowe)	0.6	TAK
Oprogramowanie do zarządzania klientami	Błąd administrowania (przypadkowe)	0.6	TAK
Oprogramowanie do zarządzania klientami	Naruszenie praw (przypadkowe)	0.6	TAK
Dane osobowe na dysku twardym	Błąd administrowania (przypadkowe)	0.5	TAK
Komputer PC	Błąd monitorowania (przypadkowe)	0.5	TAK
Drukarka	Naruszenie praw (przypadkowe)	0.5	TAK
Drukarka	Sfałszowanie oprogramowania (przypadkowe)	0.5	TAK
Windows	Błąd monitorowania (przypadkowe)	0.5	TAK
Pakiet biurowy office	Błąd użytkowania (przypadkowy)	0.5	TAK
Pakiet biurowy office	Błąd monitorowania (przypadkowe)	0.5	TAK
Oprogramowanie do zarządzania klientami	Błąd monitorowania (przypadkowe)	0.5	TAK
Wydruki papierowe	Błąd użytkowania (przypadkowy)	0.4	TAK
Drukarka	Kradzież urządzenia (umyślne)	0.3	TAK
Wydruki papierowe	Błąd administrowania (przypadkowe)	0.3	TAK
Dane osobowe na dysku twardym	Sfałszowanie oprogramowania (przypadkowe)	0.2	TAK
Komputer PC	Sfałszowanie oprogramowania (przypadkowe)	0.2	TAK
Drukarka	Błąd użytkowania (przypadkowy)	0.2	TAK
Windows	Sfałszowanie oprogramowania (przypadkowe)	0.2	TAK
Pakiet biurowy office	Sfałszowanie oprogramowania (przypadkowe)	0.2	TAK
Oprogramowanie do zarządzania klientami	Sfałszowanie oprogramowania (przypadkowe)	0.2	TAK
Dane osobowe na dysku twardym	Błąd użytkowania (przypadkowy)	0.1	TAK

DOSTEPNOŚĆ			
AKTYWA	**ZAGROŻENIA**	**RYZYKO**	**AKC**
Dysk twardy	Skasowanie informacji (umyślne)	4.0	TAK
Drukarka	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	3.8	TAK
Drukarka	Sfałszowanie oprogramowania (umyślne)	3.7	TAK
Dysk twardy	Zniszczenie urządzeń (umyślne)	3.6	TAK
Dane osobowe na dysku twardym	Zniszczenie urządzeń (umyślne)	3.5	TAK
Komputer PC	Utrata dostaw prądu (umyślne)	3.5	TAK
Drukarka	Utrata dostaw prądu (umyślne)	3.5	TAK
Dysk twardy	Manipulacja urządzeniem (umyślne)	3.5	TAK
Dysk twardy	Pożar (umyślne)	3.4	TAK
Wydruki papierowe	Pożar (umyślne)	3.4	TAK
Pomieszczenie	Wtargnięcie (umyślne)	3.4	TAK
Komputer PC	Kradzież urządzenia (umyślne)	3.1	TAK
Administrator systemu	Braki organizacyjne (przypadkowe)	3.1	TAK
Drukarka	Utrata dostaw prądu (naturalne)	3.0	TAK
Dane osobowe na dysku twardym	Kradzież nośników (umyślne)	2.9	TAK
Komputer PC	Skasowanie informacji (umyślne)	2.9	TAK
Komputer PC	Kradzież nośników (umyślne)	2.9	TAK
Dysk twardy	Kradzież nośników (umyślne)	2.9	TAK
Dane osobowe na dysku twardym	Manipulacja urządzeniem (umyślne)	2.8	TAK
Komputer PC	Zniszczenie nośników (umyślne)	2.8	TAK
Dysk twardy	Zniszczenie nośników (umyślne)	2.8	TAK

DOSTEPNOŚĆ			
AKTYWA	**ZAGROŻENIA**	**RYZYKO**	**AKC**
Komputer PC	Pożar (umyślne)	2.7	TAK
Drukarka	Pożar (umyślne)	2.7	TAK
Wydruki papierowe	Kradzież dokumentów (umyślne)	2.7	TAK
Pomieszczenie	Pożar (umyślne)	2.7	TAK
Drukarka	Manipulacja urządzeniem (umyślne)	2.6	TAK
Wydruki papierowe	Błąd administrowania (przypadkowe)	2.6	TAK
Pakiet biurowy office	Skasowanie informacji (umyślne)	2.6	TAK
Komputer PC	Manipulacja urządzeniem (umyślne)	2.5	TAK
Drukarka	Zniszczenie urządzeń (umyślne)	2.5	TAK
Windows	Skasowanie informacji (umyślne)	2.5	TAK
Dane osobowe na dysku twardym	Zniszczenie nośników (umyślne)	2.4	TAK
Komputer PC	Złośliwe oprogramowanie (umyślne)	2.4	TAK
Dysk twardy	Nieautoryzowany dostęp (umyślne)	2.4	TAK
Pakiet biurowy office	Złośliwe oprogramowanie (umyślne)	2.4	TAK
Oprogramowanie do zarządzania klientami	Złośliwe oprogramowanie (umyślne)	2.4	TAK
Dane osobowe na dysku twardym	Złośliwe oprogramowanie (umyślne)	2.3	TAK
Dane osobowe na dysku twardym	Skasowanie informacji (umyślne)	2.3	TAK
Komputer PC	Zniszczenie urządzeń (umyślne)	2.3	TAK
Drukarka	Przerwy w łączności, transmisji danych (umyślne)	2.3	TAK
Wydruki papierowe	Nieautoryzowany dostęp (umyślne)	2.3	TAK
Windows	Złośliwe oprogramowanie (umyślne)	2.3	TAK
Pomieszczenie	Nieautoryzowany dostęp (umyślne)	2.3	TAK
Dane osobowe na dysku twardym	Pożar (umyślne)	2.2	TAK
Drukarka	Błąd konfiguracyjny (przypadkowe)	2.2	TAK
Drukarka	Sfałszowanie oprogramowania (przypadkowe)	2.2	TAK
Drukarka	Błąd monitorowania (przypadkowe)	2.1	TAK
Komputer PC	Utrata dostaw prądu (naturalne)	2.0	TAK
Komputer PC	Pożar (przypadkowe)	2.0	TAK
Drukarka	Nieprawidłowa konserwacja sprzętu (przypadkowe)	2.0	TAK
Drukarka	Manipulacja konfiguracją (umyślne)	2.0	TAK
Drukarka	Pożar (przypadkowe)	2.0	TAK
Dysk twardy	Pożar (przypadkowe)	2.0	TAK
Wydruki papierowe	Pożar (przypadkowe)	2.0	TAK
Windows	Błąd konfiguracyjny (przypadkowe)	2.0	TAK
Windows	Manipulacja konfiguracją (umyślne)	2.0	TAK
Pakiet biurowy office	Manipulacja konfiguracją (umyślne)	2.0	TAK
Oprogramowanie do zarządzania klientami	Manipulacja konfiguracją (umyślne)	2.0	TAK
Pomieszczenie	Pożar (przypadkowe)	2.0	TAK
Windows	Błąd administrowania (przypadkowe)	1.9	TAK
Dane osobowe na dysku twardym	Pożar (przypadkowe)	1.8	TAK
Komputer PC	Nieprawidłowa konserwacja sprzętu (przypadkowe)	1.8	TAK
Komputer PC	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.8	TAK
Drukarka	Awaria urządzenia (przypadkowe)	1.8	TAK
Drukarka	Błąd administrowania (przypadkowe)	1.8	TAK
Drukarka	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	1.8	TAK
Windows	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.8	TAK
Dane osobowe na dysku twardym	Błąd monitorowania (przypadkowe)	1.7	TAK
Drukarka	Utrata dostaw prądu (przypadkowe)	1.7	TAK
Komputer PC	Awaria urządzenia (przypadkowe)	1.6	TAK
Komputer PC	Błąd monitorowania (przypadkowe)	1.6	TAK
Komputer PC	Błąd konfiguracyjny (przypadkowe)	1.6	TAK

DOSTEPNOŚĆ			
AKTYWA	**ZAGROŻENIA**	**RYZYKO**	**AKC**
Windows	Błąd monitorowania (przypadkowe)	1.6	TAK
Pakiet biurowy office	Błąd monitorowania (przypadkowe)	1.6	TAK
Pakiet biurowy office	Błąd konfiguracyjny (przypadkowe)	1.6	TAK
Oprogramowanie do zarządzania klientami	Błąd monitorowania (przypadkowe)	1.6	TAK
Oprogramowanie do zarządzania klientami	Błąd konfiguracyjny (przypadkowe)	1.6	TAK
Oprogramowanie do zarządzania klientami	Skasowanie informacji (umyślne)	1.6	TAK
Administrator systemu	Socjotechnika (umyślne)	1.6	TAK
Drukarka	Niewłaściwe funkcjonowanie oprogramowania (przypadkowe)	1.5	TAK
Dysk twardy	Nieprawidłowa konserwacja sprzętu (przypadkowe)	1.5	TAK
Dane osobowe na dysku twardym	Nieprawidłowa konserwacja sprzętu (przypadkowe)	1.4	TAK
Dane osobowe na dysku twardym	Sfałszowanie oprogramowania (umyślne)	1.4	TAK
Komputer PC	Pożar (naturalne)	1.4	TAK
Drukarka	Pożar (naturalne)	1.4	TAK
Dysk twardy	Pożar (naturalne)	1.4	TAK
Wydruki papierowe	Pożar (naturalne)	1.4	TAK
Windows	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	1.4	TAK
Pakiet biurowy office	Błąd administrowania (przypadkowe)	1.4	TAK
Oprogramowanie do zarządzania klientami	Błąd administrowania (przypadkowe)	1.4	TAK
Pomieszczenie	Pożar (naturalne)	1.4	TAK
Dane osobowe na dysku twardym	Błąd administrowania (przypadkowe)	1.3	TAK
Dane osobowe na dysku twardym	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.3	TAK
Komputer PC	Manipulacja konfiguracją (umyślne)	1.3	TAK
Komputer PC	Sfałszowanie oprogramowania (umyślne)	1.3	TAK
Drukarka	Nieautoryzowany dostęp (umyślne)	1.3	TAK
Windows	Sfałszowanie oprogramowania (umyślne)	1.3	TAK
Pakiet biurowy office	Sfałszowanie oprogramowania (umyślne)	1.3	TAK
Oprogramowanie do zarządzania klientami	Sfałszowanie oprogramowania (umyślne)	1.3	TAK
Dane osobowe na dysku twardym	Awaria urządzenia (przypadkowe)	1.2	TAK

INTEGRALNOŚĆ			
AKTYWA	**ZAGROŻENIA**	**RYZYKO**	**AKC**
Dysk twardy	Zmiana informacji (umyślne)	3.5	TAK
Drukarka	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	2.7	TAK
Dane osobowe na dysku twardym	Zmiana informacji (umyślne)	2.6	TAK
Pakiet biurowy office	Zmiana informacji (umyślne)	2.5	TAK
Oprogramowanie do zarządzania klientami	Zmiana informacji (umyślne)	2.5	TAK
Komputer PC	Złośliwe oprogramowanie (umyślne)	2.4	TAK
Dysk twardy	Nieautoryzowany dostęp (umyślne)	2.4	TAK
Pakiet biurowy office	Złośliwe oprogramowanie (umyślne)	2.4	TAK
Oprogramowanie do zarządzania klientami	Złośliwe oprogramowanie (umyślne)	2.4	TAK
Dane osobowe na dysku twardym	Złośliwe oprogramowanie (umyślne)	2.3	TAK
Wydruki papierowe	Nieautoryzowany dostęp (umyślne)	2.3	TAK
Windows	Złośliwe oprogramowanie (umyślne)	2.3	TAK

INTEGRALNOŚĆ			
AKTYWA	**ZAGROŻENIA**	**RYZYKO**	**AKC**
Windows	Zmiana informacji (umyślne)	2.3	TAK
Drukarka	Sfałszowanie oprogramowania (umyślne)	1.9	TAK
Drukarka	Błąd monitorowania (przypadkowe)	1.8	TAK
Komputer PC	Zmiana informacji (umyślne)	1.7	TAK
Wydruki papierowe	Błąd użytkowania (przypadkowy)	1.7	TAK
Drukarka	Sfałszowanie oprogramowania (przypadkowe)	1.5	TAK
Wydruki papierowe	Błąd administrowania (przypadkowe)	1.5	TAK
Dane osobowe na dysku twardym	Błąd monitorowania (przypadkowe)	1.4	TAK
Komputer PC	Błąd monitorowania (przypadkowe)	1.3	TAK
Komputer PC	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.3	TAK
Windows	Błąd monitorowania (przypadkowe)	1.3	TAK
Windows	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.3	TAK
Pakiet biurowy office	Błąd monitorowania (przypadkowe)	1.3	TAK
Oprogramowanie do zarządzania klientami	Błąd monitorowania (przypadkowe)	1.3	TAK
Drukarka	Błąd użytkowania (przypadkowy)	1.0	TAK
Drukarka	Błąd administrowania (przypadkowe)	1.0	TAK
Drukarka	Nieautoryzowany dostęp (umyślne)	1.0	TAK
Windows	Błąd administrowania (przypadkowe)	1.0	TAK
Windows	Manipulacja konfiguracją (umyślne)	1.0	TAK
Pakiet biurowy office	Błąd użytkowania (przypadkowy)	1.0	TAK
Pakiet biurowy office	Manipulacja konfiguracją (umyślne)	1.0	TAK
Oprogramowanie do zarządzania klientami	Manipulacja konfiguracją (umyślne)	1.0	TAK
Dane osobowe na dysku twardym	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.9	TAK
Drukarka	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.9	TAK
Dysk twardy	Zmiana informacji (przypadkowe)	0.9	TAK
Pakiet biurowy office	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.9	TAK
Oprogramowanie do zarządzania klientami	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.9	TAK
Pomieszczenie	Nieautoryzowany dostęp (umyślne)	0.9	TAK
Komputer PC	Nieautoryzowany dostęp (umyślne)	0.8	TAK
Windows	Nieautoryzowany dostęp (umyślne)	0.8	TAK
Pakiet biurowy office	Nieautoryzowany dostęp (umyślne)	0.8	TAK
Oprogramowanie do zarządzania klientami	Nieautoryzowany dostęp (umyślne)	0.8	TAK
Dane osobowe na dysku twardym	Błąd administrowania (przypadkowe)	0.7	TAK
Dane osobowe na dysku twardym	Sfałszowanie oprogramowania (przypadkowe)	0.7	TAK
Dane osobowe na dysku twardym	Sfałszowanie oprogramowania (umyślne)	0.7	TAK
Komputer PC	Błąd administrowania (przypadkowe)	0.7	TAK
Komputer PC	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.7	TAK
Komputer PC	Sfałszowanie oprogramowania (przypadkowe)	0.7	TAK
Komputer PC	Sfałszowanie oprogramowania (umyślne)	0.7	TAK
Drukarka	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.7	TAK
Windows	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.7	TAK
Windows	Sfałszowanie oprogramowania (przypadkowe)	0.7	TAK
Windows	Sfałszowanie oprogramowania (umyślne)	0.7	TAK
Pakiet biurowy office	Błąd administrowania (przypadkowe)	0.7	TAK
Pakiet biurowy office	Sfałszowanie oprogramowania (przypadkowe)	0.7	TAK
Pakiet biurowy office	Sfałszowanie oprogramowania (umyślne)	0.7	TAK

INTEGRALNOŚĆ			
AKTYWA	**ZAGROŻENIA**	**RYZYKO**	**AKC**
Oprogramowanie do zarządzania klientami	Błąd administrowania (przypadkowe)	0.7	TAK
Oprogramowanie do zarządzania klientami	Sfałszowanie oprogramowania (przypadkowe)	0.7	TAK
Oprogramowanie do zarządzania klientami	Sfałszowanie oprogramowania (umyślne)	0.7	TAK
Komputer PC	Zmiana informacji (przypadkowe)	0.6	TAK
Komputer PC	Manipulacja konfiguracją (umyślne)	0.6	TAK
Drukarka	Błąd konfiguracyjny (przypadkowe)	0.6	TAK
Dysk twardy	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.6	TAK
Windows	Błąd konfiguracyjny (przypadkowe)	0.6	TAK
Windows	Zmiana informacji (przypadkowe)	0.6	TAK
Pakiet biurowy office	Zmiana informacji (przypadkowe)	0.6	TAK
Oprogramowanie do zarządzania klientami	Zmiana informacji (przypadkowe)	0.6	TAK
Dane osobowe na dysku twardym	Błąd użytkowania (przypadkowy)	0.5	TAK
Dane osobowe na dysku twardym	Zmiana informacji (przypadkowe)	0.5	TAK
Dane osobowe na dysku twardym	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.5	TAK
Komputer PC	Błąd użytkowania (przypadkowy)	0.5	TAK
Komputer PC	Błąd konfiguracyjny (przypadkowe)	0.5	TAK
Komputer PC	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.5	TAK
Drukarka	Manipulacja konfiguracją (umyślne)	0.5	TAK
Windows	Błąd użytkowania (przypadkowy)	0.5	TAK
Pakiet biurowy office	Błąd konfiguracyjny (przypadkowe)	0.5	TAK
Pakiet biurowy office	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.5	TAK
Oprogramowanie do zarządzania klientami	Błąd użytkowania (przypadkowy)	0.5	TAK
Oprogramowanie do zarządzania klientami	Błąd konfiguracyjny (przypadkowe)	0.5	TAK
Oprogramowanie do zarządzania klientami	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.5	TAK
Administrator systemu	Socjotechnika (umyślne)	0.4	TAK
Dane osobowe na dysku twardym	Nieautoryzowany dostęp (umyślne)	0.3	TAK
Użytkownik	Socjotechnika (umyślne)	0.3	TAK

12. Wnioski

Wszystkie ryzyka utraty poufności, dostępności i integralności zasobów i danych osobowych są akceptowalne. Kierownictwo organizacji akceptuje wyniki procesu szacowania ryzyka dla bezpieczeństwa danych osobowych. Kierowniectwo organizacji akceptuje ryzyka szczątkowe wraz z jego ewentualnymi konsekwencjami.