RAPORT

ANALIZA RYZYKA

dla bezpieczeństwa danych osobowych

NOWE MIASTO

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: **NOWE MIASTO**

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
2. Dane osobowe na przenośnym nośniku pamięci
3. Dane osobowe w postaci wydruków na papierze

Dane
4. Pliki danych

Usługi
5. Hosting danych osobowych

Urządzenia przenośne
6. Laptop

Urządzenia stacjonarne
7. Komputer PC

Urządzenia peryferyjne
8. Drukarka

Nośniki elektroniczne
9. Dysk twardy
10. Pamieć FLASH (pendrive)

Inne nośniki
11. Wydruki papierowe

System operacyjny
12. Windows

Oprogramowanie standardowe
13. Pakiet biurowy office
14. Klient e-mail

Standardowe aplikacje biznesowe
15. Oprogramowanie księgowe
16. Oprogramowanie do zarządzania personelem

Media i usługi wspierające
17. WIFI
18. Sieć LAN
19. Internet

Przekaźniki aktywne i pasywne
20. Router
21. Przełącznik (switch)

Użytkownicy
22. Użytkownik

Personel ds. eksploatacji i utrzymania
23. Administrator systemu
24. Inspektor ochrony danych IOD

Siedziba
25. Pomieszczenie

Podstawowe usługi
26. Dostęp do internetu świadczony przez operatora zewnętrznego

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
10. BIOS/UEFI

Ochrona informacji/danych
11. Kopia zapasowa
12. SSL - szyfrowanie przesyłanych danych
13. Zabezpieczenie monitora przed podglądem
14. Szyfrowanie danych
15. Niszczarka dokumentów

Bezpieczeństwo osobowe / Personel
16. Szkolenia z obsługi oprogramowania dla użytkowników
17. Szkolenia z bezpieczeństwa dla użytkowników
18. Szkolenia dla administratorów
19. Szkolenia dla Inspektora Ochrony Danych
20. Lista użytkowników
21. Nadzór (nad serwisantami)
22. Nadzór (pracownicy kontraktowi)
23. Odpowiedzialność użytkowników

Ochrona usług
24. Bezpieczna telepraca

Ochrona oprogramowania
25. Regularna konserwacja i inwentaryzacja oprogramowania
26. Regularne aktualizacje systemu
27. Bezpieczna konfiguracja oprogramowania

Ochrona sprzętu
28. Sprzęt z certyfikatem CE
29. Regularna konserwacja i inwentaryzacja sprzętu
30. Zasilanie awaryjne (gwarantowane)
31. Serwis sprzętu komputerowego
32. Aktualizacja sterowników urządzeń

Ochrona komunikacji (łączności)
33. Logi bezpieczeństwa sieciowe
34. WIFI bezpieczne
35. Firewall - zapora sieciowa
36. NAT - translacja adresów sieciowych

Ochrona nośników danych
37. Konserwacja i inwentaryzacja nośników
38. Bezpieczne przechowywanie nośników
39. Niszczarka płyt CD/DVD

Bezpieczeństwo fizyczne i środowiskowe
40. Personel bezpieczeństwa w razie alarmu
41. System Sygnalizacji Włamania i Napadu SSWiN
42. System przeciwpożarowy ppoż.
43. System wentylacji
44. System klimatyzacji
45. Strefy ograniczonego dostępu
46. Ochrona kluczy do pomieszczeń (obszarów)

Organizacja
47. Plany awaryjne
48. Zarządzanie ryzykiem
49. Bieżąca kontrola
50. Dziennik Administratora Systemu
51. Współpraca zewnętrzna
52. Bezpieczny hosting danych
53. Nadzór nad zasobem/urządzeniem przez użytkownika

Procedury i polityki bezpieczeństwa
54. Procedura zarządzania zmianami sprzętu
55. Procedury zarządzania incydentami bezpieczeństwa
56. Procedura wykonywania i odtworzenia kopii danych
57. Procedura użytkowania nośników elektronicznych
58. Procedura przekazywania nośników elektronicznych
59. Procedura usuwania danych i niszczenia nośników elektronicznych
60. Procedura użytkowania stanowiska komputerowego
61. Procedura instalacji nowego oprogramowania
62. Procedura użytkowania urządzeń systemu
63. Procedura użytkowania urządzeń mobilnych
64. Polityka bezpieczeństwa
65. Procedury użytkowania poczty e-mail
66. Procedury bezpiecznego przeglądania internetu przez WWW
67. 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	5.9	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	6.2	1.9	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
Dane osobowe na przenośnym nośniku pamięci	Błąd użytkowania (przypadkowy)	0.2	1.1	0.2	TAK
Dane osobowe na przenośnym nośniku pamięci	Błąd administrowania (przypadkowe)	0.3	2.3	0.7	TAK
Dane osobowe na przenośnym nośniku pamięci	Błąd monitorowania (przypadkowe)	0.3	1.9	0.6	TAK
Dane osobowe na przenośnym nośniku pamięci	Złośliwe oprogramowanie (umyślne)	0.4	5.6	2.2	TAK
Dane osobowe na przenośnym nośniku pamięci	Ujawnienie (przypadkowe)	0.2	4.6	0.9	TAK
Dane osobowe na przenośnym nośniku pamięci	Naruszenie praw (umyślne)	0.3	4.6	1.4	TAK
Dane osobowe na przenośnym nośniku pamięci	Nieautoryzowany dostęp (umyślne)	0.2	6.0	1.2	TAK
Dane osobowe na przenośnym nośniku pamięci	Ujawnienie (umyślne)	0.3	6.1	1.8	TAK
Dane osobowe na przenośnym nośniku pamięci	Kradzież nośników (umyślne)	0.3	6.4	1.9	TAK

POUFNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Dane osobowe na przenośnym nośniku pamięci	Naruszenie praw (przypadkowe)	0.2	3.3	0.7	TAK
Dane osobowe na przenośnym nośniku pamięci	Szpiegostwo zdalne (umyślne)	0.4	4.6	1.8	TAK
Dane osobowe na przenośnym nośniku pamięci	Sfałszowanie oprogramowania (przypadkowe)	0.2	1.3	0.3	TAK
Dane osobowe na przenośnym nośniku pamięci	Sfałszowanie oprogramowania (umyślne)	0.4	5.1	2.0	TAK
Dane osobowe w postaci wydruków na papierze	Błąd użytkowania (przypadkowy)	0.3	1.3	0.4	TAK
Dane osobowe w postaci wydruków na papierze	Błąd administrowania (przypadkowe)	0.4	0.7	0.3	TAK
Dane osobowe w postaci wydruków na papierze	Ujawnienie (przypadkowe)	0.4	5.3	2.1	TAK
Dane osobowe w postaci wydruków na papierze	Nieautoryzowany dostęp (umyślne)	0.3	6.4	1.9	TAK
Dane osobowe w postaci wydruków na papierze	Ujawnienie (umyślne)	0.3	6.2	1.9	TAK
Dane osobowe w postaci wydruków na papierze	Kradzież dokumentów (umyślne)	0.4	6.3	2.5	TAK
Pliki danych	Błąd użytkowania (przypadkowy)	0.1	1.1	0.1	TAK
Pliki danych	Błąd administrowania (przypadkowe)	0.2	2.2	0.4	TAK
Pliki danych	Złośliwe oprogramowanie (umyślne)	0.3	5.1	1.5	TAK
Pliki danych	Ujawnienie (przypadkowe)	0.2	4.1	0.8	TAK
Pliki danych	Manipulacja konfiguracją (umyślne)	0.2	4.2	0.8	TAK
Pliki danych	Naruszenie praw (umyślne)	0.2	4.2	0.8	TAK
Pliki danych	Nieautoryzowany dostęp (umyślne)	0.2	5.4	1.1	TAK
Pliki danych	Ujawnienie (umyślne)	0.3	5.4	1.6	TAK
Pliki danych	Naruszenie praw (przypadkowe)	0.2	3.0	0.6	TAK
Pliki danych	Szpiegostwo zdalne (umyślne)	0.2	5.3	1.1	TAK
Pliki danych	Sfałszowanie oprogramowania (przypadkowe)	0.2	1.1	0.2	TAK
Pliki danych	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.3	5.5	1.7	TAK
Hosting danych osobowych	Ujawnienie (przypadkowe)	0.2	4.6	0.9	TAK
Hosting danych osobowych	Manipulacja konfiguracją (umyślne)	0.5	5.3	2.7	TAK
Hosting danych osobowych	Naruszenie praw (umyślne)	0.4	4.6	1.8	TAK
Hosting danych osobowych	Nieautoryzowany dostęp (umyślne)	0.3	6.5	2.0	TAK
Hosting danych osobowych	Podsłuch sieci LAN, WAN (umyślne)	0.2	4.9	1.0	TAK
Hosting danych osobowych	Ujawnienie (umyślne)	0.4	5.9	2.4	TAK
Hosting danych osobowych	Naruszenie praw (przypadkowe)	0.3	3.3	1.0	TAK
Hosting danych osobowych	Szpiegostwo zdalne (umyślne)	0.4	6.7	2.7	TAK
Laptop	Błąd użytkowania (przypadkowy)	0.1	1.1	0.1	TAK
Laptop	Błąd administrowania (przypadkowe)	0.2	3.0	0.6	TAK
Laptop	Błąd monitorowania (przypadkowe)	0.3	1.8	0.5	TAK
Laptop	Złośliwe oprogramowanie (umyślne)	0.3	5.7	1.7	TAK
Laptop	Ujawnienie (przypadkowe)	0.2	4.2	0.8	TAK
Laptop	Manipulacja konfiguracją	0.2	4.5	0.9	TAK

POUFNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
	(umyślne)				
Laptop	Naruszenie praw (umyślne)	0.2	4.2	0.8	TAK
Laptop	Nieautoryzowany dostęp (umyślne)	0.2	4.4	0.9	TAK
Laptop	Ujawnienie (umyślne)	0.3	5.0	1.5	TAK
Laptop	Kradzież nośników (umyślne)	0.2	6.0	1.2	TAK
Laptop	Naruszenie praw (przypadkowe)	0.2	3.1	0.6	TAK
Laptop	Szpiegostwo zdalne (umyślne)	0.2	6.0	1.2	TAK
Laptop	Kradzież urządzenia (umyślne)	0.3	3.8	1.1	TAK
Laptop	Sfałszowanie oprogramowania (przypadkowe)	0.2	1.1	0.2	TAK
Laptop	Sfałszowanie oprogramowania (umyślne)	0.2	4.6	0.9	TAK
Laptop	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.3	5.4	1.6	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	4.4	0.9	TAK
Komputer PC	Ujawnienie (umyślne)	0.3	5.0	1.5	TAK
Komputer PC	Kradzież nośników (umyślne)	0.2	6.0	1.2	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)	0.3	3.8	1.1	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 oprogramowania (umyślne)	0.3	5.4	1.6	TAK
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)	0.4	4.6	1.8	TAK
Drukarka	Naruszenie praw (umyślne)	0.3	3.6	1.1	TAK
Drukarka	Nieautoryzowany dostęp (umyślne)	0.2	4.7	0.9	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)	0.3	1.3	0.4	TAK
Drukarka	Sfałszowanie oprogramowania	0.5	3.2	1.6	TAK

POUFNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
	(umyślne)				
Drukarka	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.6	3.8	2.3	TAK
Dysk twardy	Ujawnienie (przypadkowe)	0.2	5.5	1.1	TAK
Dysk twardy	Nieautoryzowany dostęp (umyślne)	0.2	6.6	1.3	TAK
Dysk twardy	Ujawnienie (umyślne)	0.3	6.4	1.9	TAK
Dysk twardy	Kradzież nośników (umyślne)	0.3	6.2	1.9	TAK
Pamieć FLASH (pendrive)	Ujawnienie (przypadkowe)	0.2	5.5	1.1	TAK
Pamieć FLASH (pendrive)	Nieautoryzowany dostęp (umyślne)	0.3	6.7	2.0	TAK
Pamieć FLASH (pendrive)	Ujawnienie (umyślne)	0.3	6.4	1.9	TAK
Pamieć FLASH (pendrive)	Kradzież nośników (umyślne)	0.3	6.4	1.9	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)	0.4	5.3	2.1	TAK
Wydruki papierowe	Nieautoryzowany dostęp (umyślne)	0.3	6.4	1.9	TAK
Wydruki papierowe	Ujawnienie (umyślne)	0.3	6.2	1.9	TAK
Wydruki papierowe	Kradzież dokumentów (umyślne)	0.4	6.3	2.5	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)	0.2	4.8	1.0	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)	0.2	4.8	1.0	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
Klient e-mail	Błąd użytkowania (przypadkowy)	0.1	2.9	0.3	TAK
Klient e-mail	Błąd administrowania (przypadkowe)	0.2	3.0	0.6	TAK
Klient e-mail	Błąd monitorowania (przypadkowe)	0.2	1.8	0.4	TAK
Klient e-mail	Złośliwe oprogramowanie (umyślne)	0.3	5.5	1.7	TAK
Klient e-mail	Ujawnienie (przypadkowe)	0.2	3.6	0.7	TAK
Klient e-mail	Manipulacja konfiguracją (umyślne)	0.2	4.6	0.9	TAK
Klient e-mail	Naruszenie praw (umyślne)	0.2	4.2	0.8	TAK
Klient e-mail	Nieautoryzowany dostęp (umyślne)	0.2	5.1	1.0	TAK
Klient e-mail	Ujawnienie (umyślne)	0.3	5.3	1.6	TAK
Klient e-mail	Naruszenie praw (przypadkowe)	0.2	3.0	0.6	TAK
Klient e-mail	Szpiegostwo zdalne (umyślne)	0.2	5.2	1.0	TAK
Klient e-mail	Sfałszowanie oprogramowania (przypadkowe)	0.2	1.1	0.2	TAK
Klient e-mail	Sfałszowanie oprogramowania (umyślne)	0.2	4.6	0.9	TAK
Klient e-mail	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.2	5.4	1.1	TAK
Oprogramowanie księgowe	Błąd użytkowania (przypadkowy)	0.1	1.1	0.1	TAK
Oprogramowanie księgowe	Błąd administrowania (przypadkowe)	0.2	3.0	0.6	TAK
Oprogramowanie księgowe	Błąd monitorowania (przypadkowe)	0.3	1.8	0.5	TAK
Oprogramowanie księgowe	Złośliwe oprogramowanie (umyślne)	0.3	5.7	1.7	TAK
Oprogramowanie księgowe	Ujawnienie (przypadkowe)	0.2	3.6	0.7	TAK
Oprogramowanie księgowe	Manipulacja konfiguracją (umyślne)	0.2	4.8	1.0	TAK
Oprogramowanie księgowe	Naruszenie praw (umyślne)	0.2	4.2	0.8	TAK
Oprogramowanie księgowe	Nieautoryzowany dostęp (umyślne)	0.2	5.2	1.0	TAK
Oprogramowanie księgowe	Ujawnienie (umyślne)	0.3	5.3	1.6	TAK
Oprogramowanie księgowe	Naruszenie praw (przypadkowe)	0.2	3.1	0.6	TAK
Oprogramowanie księgowe	Szpiegostwo zdalne (umyślne)	0.2	5.4	1.1	TAK
Oprogramowanie księgowe	Sfałszowanie oprogramowania (przypadkowe)	0.2	1.1	0.2	TAK
Oprogramowanie księgowe	Sfałszowanie oprogramowania (umyślne)	0.2	4.6	0.9	TAK
Oprogramowanie księgowe	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.2	5.4	1.1	TAK
Oprogramowanie do zarządzania personelem	Błąd użytkowania (przypadkowy)	0.1	1.1	0.1	TAK
Oprogramowanie do zarządzania personelem	Błąd administrowania (przypadkowe)	0.2	3.0	0.6	TAK
Oprogramowanie do zarządzania personelem	Błąd monitorowania (przypadkowe)	0.3	1.8	0.5	TAK
Oprogramowanie do zarządzania	Złośliwe oprogramowanie	0.3	5.7	1.7	TAK

POUFNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
personelem	(umyślne)				
Oprogramowanie do zarządzania personelem	Ujawnienie (przypadkowe)	0.2	3.6	0.7	TAK
Oprogramowanie do zarządzania personelem	Manipulacja konfiguracją (umyślne)	0.2	4.8	1.0	TAK
Oprogramowanie do zarządzania personelem	Naruszenie praw (umyślne)	0.2	4.2	0.8	TAK
Oprogramowanie do zarządzania personelem	Nieautoryzowany dostęp (umyślne)	0.2	4.6	0.9	TAK
Oprogramowanie do zarządzania personelem	Ujawnienie (umyślne)	0.3	5.3	1.6	TAK
Oprogramowanie do zarządzania personelem	Naruszenie praw (przypadkowe)	0.2	3.1	0.6	TAK
Oprogramowanie do zarządzania personelem	Szpiegostwo zdalne (umyślne)	0.2	5.4	1.1	TAK
Oprogramowanie do zarządzania personelem	Sfałszowanie oprogramowania (przypadkowe)	0.2	1.1	0.2	TAK
Oprogramowanie do zarządzania personelem	Sfałszowanie oprogramowania (umyślne)	0.2	4.6	0.9	TAK
Oprogramowanie do zarządzania personelem	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.2	5.4	1.1	TAK
WIFI	Błąd użytkowania (przypadkowy)	0.1	1.1	0.1	TAK
WIFI	Błąd administrowania (przypadkowe)	0.2	5.4	1.1	TAK
WIFI	Błąd monitorowania (przypadkowe)	0.2	1.8	0.4	TAK
WIFI	Ujawnienie (przypadkowe)	0.2	3.6	0.7	TAK
WIFI	Manipulacja konfiguracją (umyślne)	0.2	4.6	0.9	TAK
WIFI	Naruszenie praw (umyślne)	0.2	4.2	0.8	TAK
WIFI	Nieautoryzowany dostęp (umyślne)	0.2	5.4	1.1	TAK
WIFI	Podsłuch sieci LAN, WAN (umyślne)	0.3	4.6	1.4	TAK
WIFI	Ujawnienie (umyślne)	0.3	5.9	1.8	TAK
WIFI	Naruszenie praw (przypadkowe)	0.2	3.0	0.6	TAK
Sieć LAN	Błąd użytkowania (przypadkowy)	0.1	0.6	0.1	TAK
Sieć LAN	Błąd administrowania (przypadkowe)	0.2	5.4	1.1	TAK
Sieć LAN	Błąd monitorowania (przypadkowe)	0.3	1.8	0.5	TAK
Sieć LAN	Ujawnienie (przypadkowe)	0.2	3.6	0.7	TAK
Sieć LAN	Manipulacja konfiguracją (umyślne)	0.2	4.4	0.9	TAK
Sieć LAN	Naruszenie praw (umyślne)	0.2	4.2	0.8	TAK
Sieć LAN	Nieautoryzowany dostęp (umyślne)	0.2	5.2	1.0	TAK
Sieć LAN	Podsłuch sieci LAN, WAN (umyślne)	0.2	4.6	0.9	TAK
Sieć LAN	Ujawnienie (umyślne)	0.2	5.0	1.0	TAK
Sieć LAN	Naruszenie praw (przypadkowe)	0.2	3.0	0.6	TAK
Sieć LAN	Szpiegostwo zdalne (umyślne)	0.2	5.3	1.1	TAK
Sieć LAN	Kradzież urządzenia (umyślne)	0.2	3.8	0.8	TAK
Internet	Złośliwe oprogramowanie (umyślne)	0.3	5.0	1.5	TAK
Internet	Ujawnienie (przypadkowe)	0.2	3.4	0.7	TAK
Internet	Naruszenie praw (umyślne)	0.2	4.0	0.8	TAK
Internet	Nieautoryzowany dostęp (umyślne)	0.2	3.6	0.7	TAK

NOWE MIASTO

POUFNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Internet	Ujawnienie (umyślne)	0.2	4.7	0.9	TAK
Internet	Szpiegostwo zdalne (umyślne)	0.2	4.3	0.9	TAK
Router	Błąd administrowania (przypadkowe)	0.3	5.5	1.7	TAK
Router	Błąd monitorowania (przypadkowe)	0.3	1.8	0.5	TAK
Router	Złośliwe oprogramowanie (umyślne)	0.3	6.2	1.9	TAK
Router	Manipulacja konfiguracją (umyślne)	0.2	0.5	0.1	TAK
Router	Naruszenie praw (umyślne)	0.2	1.9	0.4	TAK
Router	Nieautoryzowany dostęp (umyślne)	0.2	4.8	1.0	TAK
Router	Naruszenie praw (przypadkowe)	0.2	1.9	0.4	TAK
Router	Szpiegostwo zdalne (umyślne)	0.2	3.7	0.7	TAK
Router	Kradzież urządzenia (umyślne)	0.2	1.6	0.3	TAK
Przełącznik (switch)	Błąd administrowania (przypadkowe)	0.3	5.5	1.7	TAK
Przełącznik (switch)	Błąd monitorowania (przypadkowe)	0.3	1.8	0.5	TAK
Przełącznik (switch)	Złośliwe oprogramowanie (umyślne)	0.3	6.2	1.9	TAK
Przełącznik (switch)	Manipulacja konfiguracją (umyślne)	0.2	0.5	0.1	TAK
Przełącznik (switch)	Naruszenie praw (umyślne)	0.2	2.6	0.5	TAK
Przełącznik (switch)	Nieautoryzowany dostęp (umyślne)	0.2	4.8	1.0	TAK
Przełącznik (switch)	Naruszenie praw (przypadkowe)	0.2	1.9	0.4	TAK
Przełącznik (switch)	Szpiegostwo zdalne (umyślne)	0.2	3.7	0.7	TAK
Przełącznik (switch)	Kradzież urządzenia (umyślne)	0.2	1.6	0.3	TAK
Użytkownik	Ujawnienie (przypadkowe)	0.2	4.1	0.8	TAK
Użytkownik	Ujawnienie (umyślne)	0.3	5.9	1.8	TAK
Użytkownik	Socjotechnika (umyślne)	0.3	4.7	1.4	TAK
Administrator systemu	Ujawnienie (przypadkowe)	0.3	4.1	1.2	TAK
Administrator systemu	Ujawnienie (umyślne)	0.3	6.6	2.0	TAK
Administrator systemu	Socjotechnika (umyślne)	0.4	5.5	2.2	TAK
Inspektor ochrony danych IOD	Ujawnienie (przypadkowe)	0.2	4.8	1.0	TAK
Inspektor ochrony danych IOD	Ujawnienie (umyślne)	0.2	5.9	1.2	TAK
Inspektor ochrony danych IOD	Socjotechnika (umyślne)	0.3	3.4	1.0	TAK
Pomieszczenie	Nieautoryzowany dostęp (umyślne)	0.3	5.7	1.7	TAK
Pomieszczenie	Wtargnięcie (umyślne)	0.3	3.3	1.0	TAK
Dostęp do internetu świadczony przez operatora zewnętrznego	Błąd monitorowania (przypadkowe)	0.2	2.5	0.5	TAK

DOSTĘPNOŚĆ

DOSTĘPNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Dane osobowe na dysku twardym	Pożar (umyślne)	0.2	3.3	0.7	TAK
Dane osobowe na dysku twardym	Pożar (naturalne)	0.1	3.5	0.4	TAK
Dane osobowe na dysku twardym	Awaria urządzenia (przypadkowe)	0.2	6.0	1.2	TAK
Dane osobowe na dysku	Niewłaściwe funkcjonowanie	0.2	5.0	1.0	TAK

DOSTĘPNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
twardym	oprogramowania (przypadkowe)				
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	4.2	0.8	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	8.8	2.6	TAK
Dane osobowe na dysku twardym	Zniszczenie nośników (umyślne)	0.3	7.8	2.3	TAK
Dane osobowe na dysku twardym	Pożar (przypadkowe)	0.1	5.0	0.5	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
Dane osobowe na przenośnym nośniku pamięci	Pożar (umyślne)	0.4	6.3	2.5	TAK
Dane osobowe na przenośnym nośniku pamięci	Pożar (naturalne)	0.2	6.5	1.3	TAK
Dane osobowe na przenośnym nośniku pamięci	Błąd użytkowania (przypadkowy)	0.2	3.3	0.7	TAK
Dane osobowe na przenośnym nośniku pamięci	Błąd administrowania (przypadkowe)	0.3	6.6	2.0	TAK
Dane osobowe na przenośnym nośniku pamięci	Błąd monitorowania (przypadkowe)	0.3	5.5	1.7	TAK
Dane osobowe na przenośnym nośniku pamięci	Złośliwe oprogramowanie (umyślne)	0.4	8.0	3.2	TAK
Dane osobowe na przenośnym nośniku pamięci	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.2	7.0	1.4	TAK
Dane osobowe na przenośnym nośniku pamięci	Nieautoryzowany dostęp (umyślne)	0.2	4.3	0.9	TAK
Dane osobowe na przenośnym nośniku pamięci	Skasowanie informacji (umyślne)	0.3	7.8	2.3	TAK
Dane osobowe na przenośnym nośniku pamięci	Kradzież nośników (umyślne)	0.3	9.2	2.8	TAK
Dane osobowe na przenośnym nośniku pamięci	Zniszczenie nośników (umyślne)	0.3	7.9	2.4	TAK
Dane osobowe na przenośnym nośniku pamięci	Pożar (przypadkowe)	0.2	8.0	1.6	TAK
Dane osobowe na przenośnym	Manipulacja urządzeniem	0.5	6.9	3.5	TAK

DOSTĘPNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
nośniku pamięci	(umyślne)				
Dane osobowe na przenośnym nośniku pamięci	Sfałszowanie oprogramowania (przypadkowe)	0.2	5.5	1.1	TAK
Dane osobowe na przenośnym nośniku pamięci	Sfałszowanie oprogramowania (umyślne)	0.4	7.3	2.9	TAK
Dane osobowe w postaci wydruków na papierze	Pożar (umyślne)	0.2	5.8	1.2	TAK
Dane osobowe w postaci wydruków na papierze	Pożar (naturalne)	0.1	6.0	0.6	TAK
Dane osobowe w postaci wydruków na papierze	Błąd użytkowania (przypadkowy)	0.3	3.7	1.1	TAK
Dane osobowe w postaci wydruków na papierze	Błąd administrowania (przypadkowe)	0.4	6.5	2.6	TAK
Dane osobowe w postaci wydruków na papierze	Nieautoryzowany dostęp (umyślne)	0.3	4.6	1.4	TAK
Dane osobowe w postaci wydruków na papierze	Pożar (przypadkowe)	0.1	5.8	0.6	TAK
Dane osobowe w postaci wydruków na papierze	Kradzież dokumentów (umyślne)	0.4	9.0	3.6	TAK
Pliki danych	Niewłaściwe funkcjonowanie oprogramowania (przypadkowe)	0.2	5.0	1.0	TAK
Pliki danych	Błąd użytkowania (przypadkowy)	0.1	3.1	0.3	TAK
Pliki danych	Błąd administrowania (przypadkowe)	0.2	6.3	1.3	TAK
Pliki danych	Błąd konfiguracyjny (przypadkowe)	0.2	5.0	1.0	TAK
Pliki danych	Złośliwe oprogramowanie (umyślne)	0.3	7.3	2.2	TAK
Pliki danych	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.3	3.4	1.0	TAK
Pliki danych	Manipulacja konfiguracją (umyślne)	0.2	6.0	1.2	TAK
Pliki danych	Nieautoryzowany dostęp (umyślne)	0.2	5.4	1.1	TAK
Pliki danych	Skasowanie informacji (umyślne)	0.3	7.3	2.2	TAK
Pliki danych	Sfałszowanie oprogramowania (przypadkowe)	0.2	4.9	1.0	TAK
Pliki danych	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.3	6.2	1.9	TAK
Hosting danych osobowych	Awaria łączności (przypadkowe)	0.4	8.0	3.2	TAK
Hosting danych osobowych	Manipulacja konfiguracją (umyślne)	0.5	7.6	3.8	TAK
Hosting danych osobowych	Nieautoryzowany dostęp (umyślne)	0.3	4.7	1.4	TAK
Hosting danych osobowych	Skasowanie informacji (umyślne)	0.6	5.3	3.2	TAK
Hosting danych osobowych	Przerwy w łączności, transmisji danych (umyślne)	0.5	7.8	3.9	TAK
Laptop	Pożar (umyślne)	0.2	5.8	1.2	TAK
Laptop	Pożar (naturalne)	0.1	6.0	0.6	TAK
Laptop	Awaria urządzenia (przypadkowe)	0.3	5.4	1.6	TAK
Laptop	Niewłaściwe funkcjonowanie oprogramowania (przypadkowe)	0.2	5.0	1.0	TAK
Laptop	Awaria łączności (przypadkowe)	0.2	5.0	1.0	TAK
Laptop	Błąd użytkowania (przypadkowy)	0.1	3.3	0.3	TAK
Laptop	Błąd administrowania (przypadkowe)	0.2	6.0	1.2	TAK
Laptop	Błąd monitorowania (przypadkowe)	0.3	5.2	1.6	TAK

DOSTĘPNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Laptop	Błąd konfiguracyjny (przypadkowe)	0.3	5.3	1.6	TAK
Laptop	Złośliwe oprogramowanie (umyślne)	0.3	8.1	2.4	TAK
Laptop	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.2	6.1	1.2	TAK
Laptop	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.3	3.4	1.0	TAK
Laptop	Manipulacja konfiguracją (umyślne)	0.2	6.4	1.3	TAK
Laptop	Nieautoryzowany dostęp (umyślne)	0.2	5.5	1.1	TAK
Laptop	Skasowanie informacji (umyślne)	0.3	9.8	2.9	TAK
Laptop	Kradzież nośników (umyślne)	0.2	8.6	1.7	TAK
Laptop	Zniszczenie nośników (umyślne)	0.3	9.3	2.8	TAK
Laptop	Przerwy w łączności, transmisji danych (umyślne)	0.3	5.5	1.7	TAK
Laptop	Pożar (przypadkowe)	0.1	5.8	0.6	TAK
Laptop	Zniszczenie urządzeń (umyślne)	0.2	6.7	1.3	TAK
Laptop	Kradzież urządzenia (umyślne)	0.3	7.8	2.3	TAK
Laptop	Manipulacja urządzeniem (umyślne)	0.4	6.1	2.4	TAK
Laptop	Sfałszowanie oprogramowania (przypadkowe)	0.2	4.9	1.0	TAK
Laptop	Sfałszowanie oprogramowania (umyślne)	0.2	6.6	1.3	TAK
Laptop	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.3	6.0	1.8	TAK
Komputer PC	Pożar (umyślne)	0.2	5.8	1.2	TAK
Komputer PC	Pożar (naturalne)	0.1	6.0	0.6	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)	0.2	6.1	1.2	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	4.7	0.9	TAK
Komputer PC	Skasowanie informacji (umyślne)	0.3	9.8	2.9	TAK
Komputer PC	Kradzież nośników (umyślne)	0.2	8.6	1.7	TAK
Komputer PC	Utrata dostaw prądu (przypadkowe)	0.1	8.5	0.9	TAK
Komputer PC	Utrata dostaw prądu (umyślne)	0.3	9.1	2.7	TAK
Komputer PC	Zniszczenie nośników (umyślne)	0.4	9.3	3.7	TAK

DOSTĘPNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Komputer PC	Przerwy w łączności, transmisji danych (umyślne)	0.3	2.7	0.8	TAK
Komputer PC	Pożar (przypadkowe)	0.1	5.8	0.6	TAK
Komputer PC	Zniszczenie urządzeń (umyślne)	0.2	7.7	1.5	TAK
Komputer PC	Kradzież urządzenia (umyślne)	0.3	7.8	2.3	TAK
Komputer PC	Manipulacja urządzeniem (umyślne)	0.4	6.1	2.4	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)	0.2	5.8	1.2	TAK
Drukarka	Pożar (naturalne)	0.1	6.0	0.6	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)	0.1	10.0	1.0	TAK
Drukarka	Awaria łączności (przypadkowe)	0.1	3.0	0.3	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)	0.4	6.6	2.6	TAK
Drukarka	Nieautoryzowany dostęp (umyślne)	0.2	4.2	0.8	TAK
Drukarka	Skasowanie informacji (umyślne)	0.2	4.9	1.0	TAK
Drukarka	Utrata dostaw prądu (przypadkowe)	0.1	7.7	0.8	TAK
Drukarka	Utrata dostaw prądu (umyślne)	0.2	8.1	1.6	TAK
Drukarka	Przerwy w łączności, transmisji danych (umyślne)	0.5	4.5	2.3	TAK
Drukarka	Pożar (przypadkowe)	0.1	5.8	0.6	TAK
Drukarka	Zniszczenie urządzeń (umyślne)	0.2	8.2	1.6	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)	0.3	5.5	1.7	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)	0.2	5.8	1.2	TAK
Dysk twardy	Pożar (naturalne)	0.1	6.0	0.6	TAK
Dysk twardy	Awaria urządzenia (przypadkowe)	0.2	6.0	1.2	TAK
Dysk twardy	Nieprawidłowa konserwacja	0.2	7.4	1.5	TAK

DOSTĘPNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
	sprzętu (przypadkowe)				
Dysk twardy	Nieautoryzowany dostęp (umyślne)	0.2	4.7	0.9	TAK
Dysk twardy	Skasowanie informacji (umyślne)	0.3	10.0	3.0	TAK
Dysk twardy	Kradzież nośników (umyślne)	0.3	8.8	2.6	TAK
Dysk twardy	Zniszczenie nośników (umyślne)	0.3	9.3	2.8	TAK
Dysk twardy	Pożar (przypadkowe)	0.1	5.8	0.6	TAK
Dysk twardy	Zniszczenie urządzeń (umyślne)	0.4	9.1	3.6	TAK
Dysk twardy	Manipulacja urządzeniem (umyślne)	0.4	6.9	2.8	TAK
Pamieć FLASH (pendrive)	Pożar (umyślne)	0.4	8.8	3.5	TAK
Pamieć FLASH (pendrive)	Pożar (naturalne)	0.2	9.0	1.8	TAK
Pamieć FLASH (pendrive)	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.2	7.4	1.5	TAK
Pamieć FLASH (pendrive)	Nieautoryzowany dostęp (umyślne)	0.3	4.8	1.4	TAK
Pamieć FLASH (pendrive)	Skasowanie informacji (umyślne)	0.3	10.0	3.0	TAK
Pamieć FLASH (pendrive)	Kradzież nośników (umyślne)	0.3	9.2	2.8	TAK
Pamieć FLASH (pendrive)	Zniszczenie nośników (umyślne)	0.3	9.4	2.8	TAK
Pamieć FLASH (pendrive)	Pożar (przypadkowe)	0.2	8.8	1.8	TAK
Pamieć FLASH (pendrive)	Manipulacja urządzeniem (umyślne)	0.5	6.9	3.5	TAK
Wydruki papierowe	Pożar (umyślne)	0.2	5.8	1.2	TAK
Wydruki papierowe	Pożar (naturalne)	0.1	6.0	0.6	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
Wydruki papierowe	Nieautoryzowany dostęp (umyślne)	0.3	4.6	1.4	TAK
Wydruki papierowe	Pożar (przypadkowe)	0.1	5.8	0.6	TAK
Wydruki papierowe	Kradzież dokumentów (umyślne)	0.4	9.0	3.6	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)	0.3	5.1	1.5	TAK
Windows	Złośliwe oprogramowanie (umyślne)	0.3	7.7	2.3	TAK
Windows	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.3	3.4	1.0	TAK
Windows	Manipulacja konfiguracją (umyślne)	0.2	6.8	1.4	TAK
Windows	Nieautoryzowany dostęp (umyślne)	0.2	4.2	0.8	TAK
Windows	Skasowanie informacji (umyślne)	0.2	8.3	1.7	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	0.2	6.8	1.4	TAK

DOSTĘPNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
	(przypadkowe)				
Pakiet biurowy office	Błąd monitorowania (przypadkowe)	0.3	5.2	1.6	TAK
Pakiet biurowy office	Błąd konfiguracyjny (przypadkowe)	0.2	5.4	1.1	TAK
Pakiet biurowy office	Złośliwe oprogramowanie (umyślne)	0.3	8.1	2.4	TAK
Pakiet biurowy office	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.2	3.4	0.7	TAK
Pakiet biurowy office	Manipulacja konfiguracją (umyślne)	0.2	6.8	1.4	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
Klient e-mail	Niewłaściwe funkcjonowanie oprogramowania (przypadkowe)	0.2	5.0	1.0	TAK
Klient e-mail	Błąd użytkowania (przypadkowy)	0.1	3.3	0.3	TAK
Klient e-mail	Błąd administrowania (przypadkowe)	0.2	6.8	1.4	TAK
Klient e-mail	Błąd monitorowania (przypadkowe)	0.2	5.1	1.0	TAK
Klient e-mail	Błąd konfiguracyjny (przypadkowe)	0.2	5.1	1.0	TAK
Klient e-mail	Złośliwe oprogramowanie (umyślne)	0.3	7.9	2.4	TAK
Klient e-mail	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.2	3.4	0.7	TAK
Klient e-mail	Manipulacja konfiguracją (umyślne)	0.2	6.6	1.3	TAK
Klient e-mail	Nieautoryzowany dostęp (umyślne)	0.2	5.7	1.1	TAK
Klient e-mail	Skasowanie informacji (umyślne)	0.2	5.9	1.2	TAK
Klient e-mail	Sfałszowanie oprogramowania (przypadkowe)	0.2	4.9	1.0	TAK
Klient e-mail	Sfałszowanie oprogramowania (umyślne)	0.2	6.6	1.3	TAK
Klient e-mail	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.2	6.0	1.2	TAK
Oprogramowanie księgowe	Niewłaściwe funkcjonowanie oprogramowania (przypadkowe)	0.2	5.0	1.0	TAK
Oprogramowanie księgowe	Błąd użytkowania (przypadkowy)	0.1	3.3	0.3	TAK
Oprogramowanie księgowe	Błąd administrowania (przypadkowe)	0.2	6.8	1.4	TAK
Oprogramowanie księgowe	Błąd monitorowania (przypadkowe)	0.3	5.2	1.6	TAK
Oprogramowanie księgowe	Błąd konfiguracyjny (przypadkowe)	0.2	5.4	1.1	TAK
Oprogramowanie księgowe	Złośliwe oprogramowanie (umyślne)	0.3	8.1	2.4	TAK
Oprogramowanie księgowe	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.2	3.4	0.7	TAK

DOSTĘPNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Oprogramowanie księgowe	Manipulacja konfiguracją (umyślne)	0.2	6.8	1.4	TAK
Oprogramowanie księgowe	Nieautoryzowany dostęp (umyślne)	0.2	4.2	0.8	TAK
Oprogramowanie księgowe	Skasowanie informacji (umyślne)	0.2	7.8	1.6	TAK
Oprogramowanie księgowe	Sfałszowanie oprogramowania (przypadkowe)	0.2	4.9	1.0	TAK
Oprogramowanie księgowe	Sfałszowanie oprogramowania (umyślne)	0.2	6.6	1.3	TAK
Oprogramowanie księgowe	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.2	6.0	1.2	TAK
Oprogramowanie do zarządzania personelem	Niewłaściwe funkcjonowanie oprogramowania (przypadkowe)	0.2	5.0	1.0	TAK
Oprogramowanie do zarządzania personelem	Błąd użytkowania (przypadkowy)	0.1	3.3	0.3	TAK
Oprogramowanie do zarządzania personelem	Błąd administrowania (przypadkowe)	0.2	6.8	1.4	TAK
Oprogramowanie do zarządzania personelem	Błąd monitorowania (przypadkowe)	0.3	5.2	1.6	TAK
Oprogramowanie do zarządzania personelem	Błąd konfiguracyjny (przypadkowe)	0.2	5.4	1.1	TAK
Oprogramowanie do zarządzania personelem	Złośliwe oprogramowanie (umyślne)	0.3	8.1	2.4	TAK
Oprogramowanie do zarządzania personelem	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.2	3.4	0.7	TAK
Oprogramowanie do zarządzania personelem	Manipulacja konfiguracją (umyślne)	0.2	6.8	1.4	TAK
Oprogramowanie do zarządzania personelem	Nieautoryzowany dostęp (umyślne)	0.2	4.2	0.8	TAK
Oprogramowanie do zarządzania personelem	Skasowanie informacji (umyślne)	0.2	7.8	1.6	TAK
Oprogramowanie do zarządzania personelem	Sfałszowanie oprogramowania (przypadkowe)	0.2	4.9	1.0	TAK
Oprogramowanie do zarządzania personelem	Sfałszowanie oprogramowania (umyślne)	0.2	6.6	1.3	TAK
Oprogramowanie do zarządzania personelem	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.2	6.0	1.2	TAK
WIFI	Awaria łączności (przypadkowe)	0.2	9.5	1.9	TAK
WIFI	Błąd użytkowania (przypadkowy)	0.1	3.3	0.3	TAK
WIFI	Błąd administrowania (przypadkowe)	0.2	6.8	1.4	TAK
WIFI	Błąd monitorowania (przypadkowe)	0.2	5.1	1.0	TAK
WIFI	Błąd konfiguracyjny (przypadkowe)	0.2	5.0	1.0	TAK
WIFI	Manipulacja konfiguracją (umyślne)	0.2	6.6	1.3	TAK
WIFI	Nieautoryzowany dostęp (umyślne)	0.2	4.3	0.9	TAK
WIFI	Przerwy w łączności, transmisji danych (umyślne)	0.3	9.1	2.7	TAK
Sieć LAN	Pożar (umyślne)	0.4	8.8	3.5	TAK
Sieć LAN	Pożar (naturalne)	0.2	9.0	1.8	TAK
Sieć LAN	Awaria urządzenia (przypadkowe)	0.2	5.4	1.1	TAK
Sieć LAN	Niewłaściwe funkcjonowanie oprogramowania (przypadkowe)	0.2	5.0	1.0	TAK
Sieć LAN	Utrata dostaw prądu (naturalne)	0.3	10.0	3.0	TAK

DOSTĘPNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Sieć LAN	Awaria łączności (przypadkowe)	0.2	9.5	1.9	TAK
Sieć LAN	Błąd użytkowania (przypadkowy)	0.1	0.8	0.1	TAK
Sieć LAN	Błąd administrowania (przypadkowe)	0.2	6.8	1.4	TAK
Sieć LAN	Błąd monitorowania (przypadkowe)	0.3	5.1	1.5	TAK
Sieć LAN	Błąd konfiguracyjny (przypadkowe)	0.3	5.0	1.5	TAK
Sieć LAN	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.2	6.1	1.2	TAK
Sieć LAN	Manipulacja konfiguracją (umyślne)	0.2	6.2	1.2	TAK
Sieć LAN	Nieautoryzowany dostęp (umyślne)	0.2	4.1	0.8	TAK
Sieć LAN	Utrata dostaw prądu (przypadkowe)	0.2	8.7	1.7	TAK
Sieć LAN	Utrata dostaw prądu (umyślne)	0.3	9.1	2.7	TAK
Sieć LAN	Przerwy w łączności, transmisji danych (umyślne)	0.3	8.8	2.6	TAK
Sieć LAN	Pożar (przypadkowe)	0.3	8.8	2.6	TAK
Sieć LAN	Zniszczenie urządzeń (umyślne)	0.3	5.8	1.7	TAK
Sieć LAN	Kradzież urządzenia (umyślne)	0.2	5.5	1.1	TAK
Sieć LAN	Manipulacja urządzeniem (umyślne)	0.3	4.7	1.4	TAK
Internet	Awaria łączności (przypadkowe)	0.3	9.5	2.9	TAK
Internet	Złośliwe oprogramowanie (umyślne)	0.3	7.1	2.1	TAK
Internet	Nieautoryzowany dostęp (umyślne)	0.2	5.1	1.0	TAK
Internet	Skasowanie informacji (umyślne)	0.2	7.0	1.4	TAK
Router	Pożar (umyślne)	0.2	4.0	0.8	TAK
Router	Pożar (naturalne)	0.1	4.0	0.4	TAK
Router	Awaria urządzenia (przypadkowe)	0.2	5.4	1.1	TAK
Router	Niewłaściwe funkcjonowanie oprogramowania (przypadkowe)	0.3	5.0	1.5	TAK
Router	Utrata dostaw prądu (naturalne)	0.1	10.0	1.0	TAK
Router	Awaria łączności (przypadkowe)	0.1	5.7	0.6	TAK
Router	Błąd administrowania (przypadkowe)	0.3	7.0	2.1	TAK
Router	Błąd monitorowania (przypadkowe)	0.3	5.3	1.6	TAK
Router	Błąd konfiguracyjny (przypadkowe)	0.3	4.8	1.4	TAK
Router	Złośliwe oprogramowanie (umyślne)	0.3	8.9	2.7	TAK
Router	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.3	6.1	1.8	TAK
Router	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.3	3.4	1.0	TAK
Router	Manipulacja konfiguracją (umyślne)	0.2	6.2	1.2	TAK
Router	Nieautoryzowany dostęp (umyślne)	0.2	6.9	1.4	TAK
Router	Skasowanie informacji (umyślne)	0.2	5.0	1.0	TAK
Router	Utrata dostaw prądu (przypadkowe)	0.1	4.1	0.4	TAK
Router	Utrata dostaw prądu (umyślne)	0.2	4.2	0.8	TAK
Router	Przerwy w łączności, transmisji danych (umyślne)	0.3	7.1	2.1	TAK
Router	Pożar (przypadkowe)	0.1	5.6	0.6	TAK

DOSTĘPNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Router	Zniszczenie urządzeń (umyślne)	0.2	4.4	0.9	TAK
Router	Kradzież urządzenia (umyślne)	0.2	7.0	1.4	TAK
Router	Manipulacja urządzeniem (umyślne)	0.3	5.3	1.6	TAK
Przełącznik (switch)	Pożar (umyślne)	0.2	4.0	0.8	TAK
Przełącznik (switch)	Pożar (naturalne)	0.1	4.0	0.4	TAK
Przełącznik (switch)	Awaria urządzenia (przypadkowe)	0.2	5.4	1.1	TAK
Przełącznik (switch)	Niewłaściwe funkcjonowanie oprogramowania (przypadkowe)	0.3	5.0	1.5	TAK
Przełącznik (switch)	Utrata dostaw prądu (naturalne)	0.1	10.0	1.0	TAK
Przełącznik (switch)	Awaria łączności (przypadkowe)	0.1	5.7	0.6	TAK
Przełącznik (switch)	Błąd administrowania (przypadkowe)	0.3	7.0	2.1	TAK
Przełącznik (switch)	Błąd monitorowania (przypadkowe)	0.3	5.3	1.6	TAK
Przełącznik (switch)	Błąd konfiguracyjny (przypadkowe)	0.3	4.8	1.4	TAK
Przełącznik (switch)	Złośliwe oprogramowanie (umyślne)	0.3	8.9	2.7	TAK
Przełącznik (switch)	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.3	6.1	1.8	TAK
Przełącznik (switch)	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.3	3.4	1.0	TAK
Przełącznik (switch)	Manipulacja konfiguracją (umyślne)	0.2	6.2	1.2	TAK
Przełącznik (switch)	Nieautoryzowany dostęp (umyślne)	0.2	6.9	1.4	TAK
Przełącznik (switch)	Skasowanie informacji (umyślne)	0.2	5.0	1.0	TAK
Przełącznik (switch)	Utrata dostaw prądu (przypadkowe)	0.1	4.1	0.4	TAK
Przełącznik (switch)	Utrata dostaw prądu (umyślne)	0.2	4.2	0.8	TAK
Przełącznik (switch)	Przerwy w łączności, transmisji danych (umyślne)	0.3	7.1	2.1	TAK
Przełącznik (switch)	Pożar (przypadkowe)	0.1	5.6	0.6	TAK
Przełącznik (switch)	Zniszczenie urządzeń (umyślne)	0.2	6.6	1.3	TAK
Przełącznik (switch)	Kradzież urządzenia (umyślne)	0.2	7.0	1.4	TAK
Przełącznik (switch)	Manipulacja urządzeniem (umyślne)	0.3	5.3	1.6	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
Inspektor ochrony danych IOD	Braki organizacyjne (przypadkowe)	0.5	6.2	3.1	TAK
Inspektor ochrony danych IOD	Naruszenie dostępności personelu (przypadkowe)	0.1	4.3	0.4	TAK
Inspektor ochrony danych IOD	Socjotechnika (umyślne)	0.3	2.0	0.6	TAK
Pomieszczenie	Pożar (umyślne)	0.2	5.8	1.2	TAK
Pomieszczenie	Pożar (naturalne)	0.1	6.0	0.6	TAK
Pomieszczenie	Nieautoryzowany dostęp (umyślne)	0.3	4.6	1.4	TAK
Pomieszczenie	Wtargnięcie (umyślne)	0.3	9.4	2.8	TAK
Pomieszczenie	Pożar (przypadkowe)	0.1	5.8	0.6	TAK
Dostęp do internetu świadczony przez operatora zewnętrznego	Awaria łączności (przypadkowe)	0.4	9.5	3.8	TAK

NOWE MIASTO

DOSTĘPNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Dostęp do internetu świadczony przez operatora zewnętrznego	Błąd monitorowania (przypadkowe)	0.2	8.1	1.6	TAK
Dostęp do internetu świadczony przez operatora zewnętrznego	Błąd konfiguracyjny (przypadkowe)	0.2	5.4	1.1	TAK
Dostęp do internetu świadczony przez operatora zewnętrznego	Przerwy w łączności, transmisji danych (umyślne)	0.4	9.1	3.6	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)	0.1	2.7	0.3	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
Dane osobowe na przenośnym nośniku pamięci	Błąd użytkowania (przypadkowy)	0.2	4.9	1.0	TAK
Dane osobowe na przenośnym nośniku pamięci	Błąd administrowania (przypadkowe)	0.3	3.3	1.0	TAK
Dane osobowe na przenośnym nośniku pamięci	Błąd monitorowania (przypadkowe)	0.3	4.6	1.4	TAK
Dane osobowe na przenośnym nośniku pamięci	Złośliwe oprogramowanie (umyślne)	0.4	8.0	3.2	TAK
Dane osobowe na przenośnym nośniku pamięci	Zmiana informacji (przypadkowe)	0.2	2.7	0.5	TAK
Dane osobowe na przenośnym nośniku pamięci	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.2	2.6	0.5	TAK
Dane osobowe na przenośnym nośniku pamięci	Nieautoryzowany dostęp (umyślne)	0.2	1.7	0.3	TAK
Dane osobowe na przenośnym nośniku pamięci	Zmiana informacji (umyślne)	0.3	8.5	2.6	TAK
Dane osobowe na przenośnym nośniku pamięci	Sfałszowanie oprogramowania (przypadkowe)	0.2	3.6	0.7	TAK
Dane osobowe na przenośnym nośniku pamięci	Sfałszowanie oprogramowania (umyślne)	0.4	3.6	1.4	TAK

INTEGRALNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Dane osobowe w postaci wydruków na papierze	Błąd użytkowania (przypadkowy)	0.3	5.5	1.7	TAK
Dane osobowe w postaci wydruków na papierze	Błąd administrowania (przypadkowe)	0.4	3.7	1.5	TAK
Dane osobowe w postaci wydruków na papierze	Nieautoryzowany dostęp (umyślne)	0.3	4.6	1.4	TAK
Pliki danych	Błąd użytkowania (przypadkowy)	0.1	4.6	0.5	TAK
Pliki danych	Błąd administrowania (przypadkowe)	0.2	3.2	0.6	TAK
Pliki danych	Błąd konfiguracyjny (przypadkowe)	0.2	1.4	0.3	TAK
Pliki danych	Złośliwe oprogramowanie (umyślne)	0.3	7.3	2.2	TAK
Pliki danych	Zmiana informacji (przypadkowe)	0.1	2.6	0.3	TAK
Pliki danych	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.3	1.7	0.5	TAK
Pliki danych	Manipulacja konfiguracją (umyślne)	0.2	3.0	0.6	TAK
Pliki danych	Nieautoryzowany dostęp (umyślne)	0.2	5.4	1.1	TAK
Pliki danych	Zmiana informacji (umyślne)	0.3	7.7	2.3	TAK
Pliki danych	Sfałszowanie oprogramowania (przypadkowe)	0.2	3.3	0.7	TAK
Pliki danych	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.3	4.4	1.3	TAK
Hosting danych osobowych	Zmiana informacji (przypadkowe)	0.2	2.6	0.5	TAK
Hosting danych osobowych	Manipulacja konfiguracją (umyślne)	0.5	3.8	1.9	TAK
Hosting danych osobowych	Nieautoryzowany dostęp (umyślne)	0.3	4.7	1.4	TAK
Hosting danych osobowych	Zmiana informacji (umyślne)	0.4	7.7	3.1	TAK
Laptop	Błąd użytkowania (przypadkowy)	0.1	4.9	0.5	TAK
Laptop	Błąd administrowania (przypadkowe)	0.2	3.4	0.7	TAK
Laptop	Błąd monitorowania (przypadkowe)	0.3	4.4	1.3	TAK
Laptop	Błąd konfiguracyjny (przypadkowe)	0.3	1.5	0.5	TAK
Laptop	Złośliwe oprogramowanie (umyślne)	0.3	8.1	2.4	TAK
Laptop	Zmiana informacji (przypadkowe)	0.1	3.0	0.3	TAK
Laptop	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.2	2.3	0.5	TAK
Laptop	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.3	1.7	0.5	TAK
Laptop	Manipulacja konfiguracją (umyślne)	0.2	3.2	0.6	TAK
Laptop	Nieautoryzowany dostęp (umyślne)	0.2	4.0	0.8	TAK
Laptop	Zmiana informacji (umyślne)	0.2	8.3	1.7	TAK
Laptop	Sfałszowanie oprogramowania (przypadkowe)	0.2	3.3	0.7	TAK
Laptop	Sfałszowanie oprogramowania (umyślne)	0.2	3.3	0.7	TAK
Laptop	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.3	4.3	1.3	TAK
Komputer PC	Błąd użytkowania (przypadkowy)	0.1	4.9	0.5	TAK
Komputer PC	Błąd administrowania	0.2	3.4	0.7	TAK

INTEGRALNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
	(przypadkowe)				
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
Komputer PC	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.2	2.3	0.5	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)	0.4	1.6	0.6	TAK
Drukarka	Nieautoryzowany dostęp (umyślne)	0.2	3.4	0.7	TAK
Drukarka	Sfałszowanie oprogramowania (przypadkowe)	0.3	3.7	1.1	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)	0.2	4.7	0.9	TAK
Dysk twardy	Zmiana informacji (umyślne)	0.5	7.0	3.5	TAK
Pamieć FLASH (pendrive)	Zmiana informacji (przypadkowe)	0.2	3.0	0.6	TAK
Pamieć FLASH (pendrive)	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.2	2.8	0.6	TAK
Pamieć FLASH (pendrive)	Nieautoryzowany dostęp (umyślne)	0.3	4.8	1.4	TAK
Pamieć FLASH (pendrive)	Zmiana informacji (umyślne)	0.4	8.0	3.2	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

INTEGRALNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Wydruki papierowe	Nieautoryzowany dostęp (umyślne)	0.3	4.6	1.4	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)	0.3	1.5	0.5	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)	0.3	1.7	0.5	TAK
Windows	Manipulacja konfiguracją (umyślne)	0.2	3.4	0.7	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
Pakiet biurowy office	Błąd monitorowania (przypadkowe)	0.3	4.4	1.3	TAK
Pakiet biurowy office	Błąd konfiguracyjny (przypadkowe)	0.2	1.5	0.3	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)	0.2	1.7	0.3	TAK
Pakiet biurowy office	Manipulacja konfiguracją (umyślne)	0.2	3.4	0.7	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
Klient e-mail	Błąd użytkowania (przypadkowy)	0.1	4.9	0.5	TAK
Klient e-mail	Błąd administrowania (przypadkowe)	0.2	3.4	0.7	TAK
Klient e-mail	Błąd monitorowania (przypadkowe)	0.2	4.3	0.9	TAK
Klient e-mail	Błąd konfiguracyjny (przypadkowe)	0.2	1.5	0.3	TAK
Klient e-mail	Złośliwe oprogramowanie (umyślne)	0.3	7.9	2.4	TAK
Klient e-mail	Zmiana informacji (przypadkowe)	0.2	3.0	0.6	TAK

INTEGRALNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Klient e-mail	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.2	1.7	0.3	TAK
Klient e-mail	Manipulacja konfiguracją (umyślne)	0.2	3.3	0.7	TAK
Klient e-mail	Nieautoryzowany dostęp (umyślne)	0.2	1.6	0.3	TAK
Klient e-mail	Zmiana informacji (umyślne)	0.3	8.3	2.5	TAK
Klient e-mail	Sfałszowanie oprogramowania (przypadkowe)	0.2	3.3	0.7	TAK
Klient e-mail	Sfałszowanie oprogramowania (umyślne)	0.2	3.3	0.7	TAK
Klient e-mail	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.2	4.3	0.9	TAK
Oprogramowanie księgowe	Błąd użytkowania (przypadkowy)	0.1	4.9	0.5	TAK
Oprogramowanie księgowe	Błąd administrowania (przypadkowe)	0.2	3.4	0.7	TAK
Oprogramowanie księgowe	Błąd monitorowania (przypadkowe)	0.3	4.4	1.3	TAK
Oprogramowanie księgowe	Błąd konfiguracyjny (przypadkowe)	0.2	1.5	0.3	TAK
Oprogramowanie księgowe	Złośliwe oprogramowanie (umyślne)	0.3	8.1	2.4	TAK
Oprogramowanie księgowe	Zmiana informacji (przypadkowe)	0.2	3.0	0.6	TAK
Oprogramowanie księgowe	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.2	1.7	0.3	TAK
Oprogramowanie księgowe	Manipulacja konfiguracją (umyślne)	0.2	3.4	0.7	TAK
Oprogramowanie księgowe	Nieautoryzowany dostęp (umyślne)	0.2	4.2	0.8	TAK
Oprogramowanie księgowe	Zmiana informacji (umyślne)	0.3	8.3	2.5	TAK
Oprogramowanie księgowe	Sfałszowanie oprogramowania (przypadkowe)	0.2	3.3	0.7	TAK
Oprogramowanie księgowe	Sfałszowanie oprogramowania (umyślne)	0.2	3.3	0.7	TAK
Oprogramowanie księgowe	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.2	4.3	0.9	TAK
Oprogramowanie do zarządzania personelem	Błąd użytkowania (przypadkowy)	0.1	4.9	0.5	TAK
Oprogramowanie do zarządzania personelem	Błąd administrowania (przypadkowe)	0.2	3.4	0.7	TAK
Oprogramowanie do zarządzania personelem	Błąd monitorowania (przypadkowe)	0.3	4.4	1.3	TAK
Oprogramowanie do zarządzania personelem	Błąd konfiguracyjny (przypadkowe)	0.2	1.5	0.3	TAK
Oprogramowanie do zarządzania personelem	Złośliwe oprogramowanie (umyślne)	0.3	8.1	2.4	TAK
Oprogramowanie do zarządzania personelem	Zmiana informacji (przypadkowe)	0.2	3.0	0.6	TAK
Oprogramowanie do zarządzania personelem	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.2	1.7	0.3	TAK
Oprogramowanie do zarządzania personelem	Manipulacja konfiguracją (umyślne)	0.2	3.4	0.7	TAK
Oprogramowanie do zarządzania personelem	Nieautoryzowany dostęp (umyślne)	0.2	4.2	0.8	TAK
Oprogramowanie do zarządzania personelem	Zmiana informacji (umyślne)	0.3	8.3	2.5	TAK
Oprogramowanie do zarządzania	Sfałszowanie oprogramowania	0.2	3.3	0.7	TAK

INTEGRALNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
personelem	(przypadkowe)				
Oprogramowanie do zarządzania personelem	Sfałszowanie oprogramowania (umyślne)	0.2	3.3	0.7	TAK
Oprogramowanie do zarządzania personelem	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.2	4.3	0.9	TAK
WIFI	Błąd użytkowania (przypadkowy)	0.1	0.8	0.1	TAK
WIFI	Błąd administrowania (przypadkowe)	0.2	3.4	0.7	TAK
WIFI	Błąd monitorowania (przypadkowe)	0.2	4.3	0.9	TAK
WIFI	Błąd konfiguracyjny (przypadkowe)	0.2	1.4	0.3	TAK
WIFI	Manipulacja konfiguracją (umyślne)	0.2	0.8	0.2	TAK
WIFI	Nieautoryzowany dostęp (umyślne)	0.2	1.7	0.3	TAK
Sieć LAN	Błąd użytkowania (przypadkowy)	0.1	0.8	0.1	TAK
Sieć LAN	Błąd administrowania (przypadkowe)	0.2	3.4	0.7	TAK
Sieć LAN	Błąd monitorowania (przypadkowe)	0.3	4.3	1.3	TAK
Sieć LAN	Błąd konfiguracyjny (przypadkowe)	0.3	1.4	0.4	TAK
Sieć LAN	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.2	2.3	0.5	TAK
Sieć LAN	Manipulacja konfiguracją (umyślne)	0.2	3.1	0.6	TAK
Sieć LAN	Nieautoryzowany dostęp (umyślne)	0.2	1.6	0.3	TAK
Internet	Złośliwe oprogramowanie (umyślne)	0.3	7.1	2.1	TAK
Internet	Nieautoryzowany dostęp (umyślne)	0.2	1.5	0.3	TAK
Internet	Zmiana informacji (umyślne)	0.3	7.4	2.2	TAK
Router	Błąd administrowania (przypadkowe)	0.3	3.5	1.1	TAK
Router	Błąd monitorowania (przypadkowe)	0.3	4.4	1.3	TAK
Router	Błąd konfiguracyjny (przypadkowe)	0.3	1.4	0.4	TAK
Router	Złośliwe oprogramowanie (umyślne)	0.3	8.9	2.7	TAK
Router	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.3	2.3	0.7	TAK
Router	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.3	1.7	0.5	TAK
Router	Manipulacja konfiguracją (umyślne)	0.2	0.8	0.2	TAK
Router	Nieautoryzowany dostęp (umyślne)	0.2	1.7	0.3	TAK
Przełącznik (switch)	Błąd administrowania (przypadkowe)	0.3	3.5	1.1	TAK
Przełącznik (switch)	Błąd monitorowania (przypadkowe)	0.3	4.4	1.3	TAK
Przełącznik (switch)	Błąd konfiguracyjny (przypadkowe)	0.3	1.4	0.4	TAK
Przełącznik (switch)	Złośliwe oprogramowanie (umyślne)	0.3	8.9	2.7	TAK
Przełącznik (switch)	Nieprawidłowa konserwacja sprzętu (przypadkowe)	0.3	2.3	0.7	TAK

INTEGRALNOŚĆ					
AKTYWA	**ZAGROŻENIA**	**PRAW.**	**SKUTKI**	**RYZYKO**	**AKC**
Przełącznik (switch)	Nieprawidłowa konserwacja oprogramowania (przypadkowe)	0.3	1.7	0.5	TAK
Przełącznik (switch)	Manipulacja konfiguracją (umyślne)	0.2	0.8	0.2	TAK
Przełącznik (switch)	Nieautoryzowany dostęp (umyślne)	0.2	1.7	0.3	TAK
Użytkownik	Socjotechnika (umyślne)	0.3	1.0	0.3	TAK
Administrator systemu	Socjotechnika (umyślne)	0.4	1.0	0.4	TAK
Inspektor ochrony danych IOD	Socjotechnika (umyślne)	0.3	1.0	0.3	TAK
Pomieszczenie	Nieautoryzowany dostęp (umyślne)	0.3	1.8	0.5	TAK
Dostęp do internetu świadczony przez operatora zewnętrznego	Błąd monitorowania (przypadkowe)	0.2	4.5	0.9	TAK
Dostęp do internetu świadczony przez operatora zewnętrznego	Błąd konfiguracyjny (przypadkowe)	0.2	1.5	0.3	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**
Hosting danych osobowych	Manipulacja konfiguracją (umyślne)	2.7	TAK
Hosting danych osobowych	Szpiegostwo zdalne (umyślne)	2.7	TAK
Dane osobowe w postaci wydruków na papierze	Kradzież dokumentów (umyślne)	2.5	TAK
Wydruki papierowe	Kradzież dokumentów (umyślne)	2.5	TAK
Hosting danych osobowych	Ujawnienie (umyślne)	2.4	TAK
Drukarka	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	2.3	TAK
Dane osobowe na przenośnym nośniku pamięci	Złośliwe oprogramowanie (umyślne)	2.2	TAK
Administrator systemu	Socjotechnika (umyślne)	2.2	TAK
Dane osobowe w postaci wydruków na papierze	Ujawnienie (przypadkowe)	2.1	TAK
Wydruki papierowe	Ujawnienie (przypadkowe)	2.1	TAK
Dane osobowe na przenośnym nośniku pamięci	Sfałszowanie oprogramowania (umyślne)	2.0	TAK
Hosting danych osobowych	Nieautoryzowany dostęp (umyślne)	2.0	TAK
Pamieć FLASH (pendrive)	Nieautoryzowany dostęp (umyślne)	2.0	TAK
Administrator systemu	Ujawnienie (umyślne)	2.0	TAK
Dane osobowe na dysku twardym	Kradzież nośników (umyślne)	1.9	TAK
Dane osobowe na przenośnym nośniku pamięci	Kradzież nośników (umyślne)	1.9	TAK
Dane osobowe w postaci wydruków na papierze	Nieautoryzowany dostęp (umyślne)	1.9	TAK
Dane osobowe w postaci wydruków na papierze	Ujawnienie (umyślne)	1.9	TAK
Dysk twardy	Ujawnienie (umyślne)	1.9	TAK
Dysk twardy	Kradzież nośników (umyślne)	1.9	TAK
Pamieć FLASH (pendrive)	Ujawnienie (umyślne)	1.9	TAK
Pamieć FLASH (pendrive)	Kradzież nośników (umyślne)	1.9	TAK
Wydruki papierowe	Nieautoryzowany dostęp (umyślne)	1.9	TAK
Wydruki papierowe	Ujawnienie (umyślne)	1.9	TAK
Router	Złośliwe oprogramowanie (umyślne)	1.9	TAK

POUFNOŚĆ			
AKTYWA	**ZAGROŻENIA**	**RYZYKO**	**AKC**
Przełącznik (switch)	Złośliwe oprogramowanie (umyślne)	1.9	TAK
Dane osobowe na dysku twardym	Ujawnienie (umyślne)	1.8	TAK
Dane osobowe na przenośnym nośniku pamięci	Ujawnienie (umyślne)	1.8	TAK
Dane osobowe na przenośnym nośniku pamięci	Szpiegostwo zdalne (umyślne)	1.8	TAK
Hosting danych osobowych	Naruszenie praw (umyślne)	1.8	TAK
Drukarka	Manipulacja konfiguracją (umyślne)	1.8	TAK
WIFI	Ujawnienie (umyślne)	1.8	TAK
Użytkownik	Ujawnienie (umyślne)	1.8	TAK
Dane osobowe na dysku twardym	Złośliwe oprogramowanie (umyślne)	1.7	TAK
Pliki danych	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.7	TAK
Laptop	Złośliwe oprogramowanie (umyślne)	1.7	TAK
Komputer PC	Złośliwe oprogramowanie (umyślne)	1.7	TAK
Pakiet biurowy office	Złośliwe oprogramowanie (umyślne)	1.7	TAK
Klient e-mail	Złośliwe oprogramowanie (umyślne)	1.7	TAK
Oprogramowanie księgowe	Złośliwe oprogramowanie (umyślne)	1.7	TAK
Oprogramowanie do zarządzania personelem	Złośliwe oprogramowanie (umyślne)	1.7	TAK
Router	Błąd administrowania (przypadkowe)	1.7	TAK
Przełącznik (switch)	Błąd administrowania (przypadkowe)	1.7	TAK
Pomieszczenie	Nieautoryzowany dostęp (umyślne)	1.7	TAK
Pliki danych	Ujawnienie (umyślne)	1.6	TAK
Laptop	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.6	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
Klient e-mail	Ujawnienie (umyślne)	1.6	TAK
Oprogramowanie księgowe	Ujawnienie (umyślne)	1.6	TAK
Oprogramowanie do zarządzania personelem	Ujawnienie (umyślne)	1.6	TAK
Pliki danych	Złośliwe oprogramowanie (umyślne)	1.5	TAK
Laptop	Ujawnienie (umyślne)	1.5	TAK
Komputer PC	Ujawnienie (umyślne)	1.5	TAK
Internet	Złośliwe oprogramowanie (umyślne)	1.5	TAK
Dane osobowe na przenośnym nośniku pamięci	Naruszenie praw (umyślne)	1.4	TAK
WIFI	Podsłuch sieci LAN, WAN (umyślne)	1.4	TAK
Użytkownik	Socjotechnika (umyślne)	1.4	TAK
Drukarka	Ujawnienie (umyślne)	1.3	TAK
Dysk twardy	Nieautoryzowany dostęp (umyślne)	1.3	TAK
Dane osobowe na dysku twardym	Nieautoryzowany dostęp (umyślne)	1.2	TAK
Dane osobowe na przenośnym nośniku pamięci	Nieautoryzowany dostęp (umyślne)	1.2	TAK
Laptop	Kradzież nośników (umyślne)	1.2	TAK
Laptop	Szpiegostwo zdalne (umyślne)	1.2	TAK
Komputer PC	Kradzież nośników (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

POUFNOŚĆ			
AKTYWA	**ZAGROŻENIA**	**RYZYKO**	**AKC**
Administrator systemu	Ujawnienie (przypadkowe)	1.2	TAK
Inspektor ochrony danych IOD	Ujawnienie (umyślne)	1.2	TAK
Dane osobowe na dysku twardym	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.1	TAK
Pliki danych	Nieautoryzowany dostęp (umyślne)	1.1	TAK
Pliki danych	Szpiegostwo zdalne (umyślne)	1.1	TAK
Laptop	Kradzież urządzenia (umyślne)	1.1	TAK
Komputer PC	Kradzież urządzenia (umyślne)	1.1	TAK
Drukarka	Naruszenie praw (umyślne)	1.1	TAK
Dysk twardy	Ujawnienie (przypadkowe)	1.1	TAK
Pamieć FLASH (pendrive)	Ujawnienie (przypadkowe)	1.1	TAK
Pakiet biurowy office	Szpiegostwo zdalne (umyślne)	1.1	TAK
Pakiet biurowy office	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.1	TAK
Klient e-mail	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.1	TAK
Oprogramowanie księgowe	Szpiegostwo zdalne (umyślne)	1.1	TAK
Oprogramowanie księgowe	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.1	TAK
Oprogramowanie do zarządzania personelem	Szpiegostwo zdalne (umyślne)	1.1	TAK
Oprogramowanie do zarządzania personelem	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.1	TAK
WIFI	Błąd administrowania (przypadkowe)	1.1	TAK
WIFI	Nieautoryzowany dostęp (umyślne)	1.1	TAK
Sieć LAN	Błąd administrowania (przypadkowe)	1.1	TAK
Sieć LAN	Szpiegostwo zdalne (umyślne)	1.1	TAK
Dane osobowe na dysku twardym	Sfałszowanie oprogramowania (umyślne)	1.0	TAK
Hosting danych osobowych	Podsłuch sieci LAN, WAN (umyślne)	1.0	TAK
Hosting danych osobowych	Naruszenie praw (przypadkowe)	1.0	TAK
Windows	Manipulacja konfiguracją (umyślne)	1.0	TAK
Windows	Nieautoryzowany dostęp (umyślne)	1.0	TAK
Pakiet biurowy office	Manipulacja konfiguracją (umyślne)	1.0	TAK
Klient e-mail	Nieautoryzowany dostęp (umyślne)	1.0	TAK
Klient e-mail	Szpiegostwo zdalne (umyślne)	1.0	TAK

DOSTEPNOŚĆ			
AKTYWA	**ZAGROŻENIA**	**RYZYKO**	**AKC**
Hosting danych osobowych	Przerwy w łączności, transmisji danych (umyślne)	3.9	TAK
Hosting danych osobowych	Manipulacja konfiguracją (umyślne)	3.8	TAK
Drukarka	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	3.8	TAK
Dostęp do internetu świadczony przez operatora zewnętrznego	Awaria łączności (przypadkowe)	3.8	TAK
Komputer PC	Zniszczenie nośników (umyślne)	3.7	TAK
Drukarka	Sfałszowanie oprogramowania (umyślne)	3.7	TAK
Dane osobowe w postaci wydruków na papierze	Kradzież dokumentów (umyślne)	3.6	TAK
Dysk twardy	Zniszczenie urządzeń (umyślne)	3.6	TAK
Wydruki papierowe	Kradzież dokumentów (umyślne)	3.6	TAK
Dostęp do internetu świadczony przez operatora zewnętrznego	Przerwy w łączności, transmisji danych (umyślne)	3.6	TAK
Dane osobowe na dysku twardym	Zniszczenie urządzeń (umyślne)	3.5	TAK

DOSTEPNOŚĆ			
AKTYWA	**ZAGROŻENIA**	**RYZYKO**	**AKC**
Dane osobowe na przenośnym nośniku pamięci	Manipulacja urządzeniem (umyślne)	3.5	TAK
Pamieć FLASH (pendrive)	Pożar (umyślne)	3.5	TAK
Pamieć FLASH (pendrive)	Manipulacja urządzeniem (umyślne)	3.5	TAK
Sieć LAN	Pożar (umyślne)	3.5	TAK
Dane osobowe na przenośnym nośniku pamięci	Złośliwe oprogramowanie (umyślne)	3.2	TAK
Hosting danych osobowych	Awaria łączności (przypadkowe)	3.2	TAK
Hosting danych osobowych	Skasowanie informacji (umyślne)	3.2	TAK
Administrator systemu	Braki organizacyjne (przypadkowe)	3.1	TAK
Inspektor ochrony danych IOD	Braki organizacyjne (przypadkowe)	3.1	TAK
Dysk twardy	Skasowanie informacji (umyślne)	3.0	TAK
Pamieć FLASH (pendrive)	Skasowanie informacji (umyślne)	3.0	TAK
Sieć LAN	Utrata dostaw prądu (naturalne)	3.0	TAK
Dane osobowe na przenośnym nośniku pamięci	Sfałszowanie oprogramowania (umyślne)	2.9	TAK
Laptop	Skasowanie informacji (umyślne)	2.9	TAK
Komputer PC	Skasowanie informacji (umyślne)	2.9	TAK
Internet	Awaria łączności (przypadkowe)	2.9	TAK
Dane osobowe na dysku twardym	Manipulacja urządzeniem (umyślne)	2.8	TAK
Dane osobowe na przenośnym nośniku pamięci	Kradzież nośników (umyślne)	2.8	TAK
Laptop	Zniszczenie nośników (umyślne)	2.8	TAK
Dysk twardy	Zniszczenie nośników (umyślne)	2.8	TAK
Dysk twardy	Manipulacja urządzeniem (umyślne)	2.8	TAK
Pamieć FLASH (pendrive)	Kradzież nośników (umyślne)	2.8	TAK
Pamieć FLASH (pendrive)	Zniszczenie nośników (umyślne)	2.8	TAK
Pomieszczenie	Wtargnięcie (umyślne)	2.8	TAK
Komputer PC	Utrata dostaw prądu (umyślne)	2.7	TAK
WIFI	Przerwy w łączności, transmisji danych (umyślne)	2.7	TAK
Sieć LAN	Utrata dostaw prądu (umyślne)	2.7	TAK
Router	Złośliwe oprogramowanie (umyślne)	2.7	TAK
Przełącznik (switch)	Złośliwe oprogramowanie (umyślne)	2.7	TAK
Dane osobowe na dysku twardym	Kradzież nośników (umyślne)	2.6	TAK
Dane osobowe w postaci wydruków na papierze	Błąd administrowania (przypadkowe)	2.6	TAK
Drukarka	Manipulacja konfiguracją (umyślne)	2.6	TAK
Drukarka	Manipulacja urządzeniem (umyślne)	2.6	TAK
Dysk twardy	Kradzież nośników (umyślne)	2.6	TAK
Wydruki papierowe	Błąd administrowania (przypadkowe)	2.6	TAK
Pakiet biurowy office	Skasowanie informacji (umyślne)	2.6	TAK
Sieć LAN	Przerwy w łączności, transmisji danych (umyślne)	2.6	TAK
Sieć LAN	Pożar (przypadkowe)	2.6	TAK
Dane osobowe na przenośnym nośniku pamięci	Pożar (umyślne)	2.5	TAK
Dane osobowe na przenośnym nośniku pamięci	Zniszczenie nośników (umyślne)	2.4	TAK
Laptop	Złośliwe oprogramowanie (umyślne)	2.4	TAK
Laptop	Manipulacja urządzeniem (umyślne)	2.4	TAK
Komputer PC	Złośliwe oprogramowanie (umyślne)	2.4	TAK
Komputer PC	Manipulacja urządzeniem (umyślne)	2.4	TAK
Pakiet biurowy office	Złośliwe oprogramowanie (umyślne)	2.4	TAK
Klient e-mail	Złośliwe oprogramowanie (umyślne)	2.4	TAK
Oprogramowanie księgowe	Złośliwe oprogramowanie (umyślne)	2.4	TAK

DOSTEPNOŚĆ			
AKTYWA	**ZAGROŻENIA**	**RYZYKO**	**AKC**
Oprogramowanie do zarządzania personelem	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
Dane osobowe na dysku twardym	Zniszczenie nośników (umyślne)	2.3	TAK
Dane osobowe na przenośnym nośniku pamięci	Skasowanie informacji (umyślne)	2.3	TAK
Laptop	Kradzież urządzenia (umyślne)	2.3	TAK
Komputer PC	Kradzież urządzenia (umyślne)	2.3	TAK
Drukarka	Przerwy w łączności, transmisji danych (umyślne)	2.3	TAK
Windows	Złośliwe oprogramowanie (umyślne)	2.3	TAK
Pliki danych	Złośliwe oprogramowanie (umyślne)	2.2	TAK
Pliki danych	Skasowanie informacji (umyślne)	2.2	TAK
Drukarka	Błąd konfiguracyjny (przypadkowe)	2.2	TAK
Drukarka	Błąd monitorowania (przypadkowe)	2.1	TAK
Internet	Złośliwe oprogramowanie (umyślne)	2.1	TAK
Router	Błąd administrowania (przypadkowe)	2.1	TAK
Router	Przerwy w łączności, transmisji danych (umyślne)	2.1	TAK
Przełącznik (switch)	Błąd administrowania (przypadkowe)	2.1	TAK
Przełącznik (switch)	Przerwy w łączności, transmisji danych (umyślne)	2.1	TAK
Dane osobowe na przenośnym nośniku pamięci	Błąd administrowania (przypadkowe)	2.0	TAK
Komputer PC	Utrata dostaw prądu (naturalne)	2.0	TAK
Drukarka	Nieprawidłowa konserwacja sprzętu (przypadkowe)	2.0	TAK
Pliki danych	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.9	TAK
Windows	Błąd administrowania (przypadkowe)	1.9	TAK
WIFI	Awaria łączności (przypadkowe)	1.9	TAK
Sieć LAN	Awaria łączności (przypadkowe)	1.9	TAK
Laptop	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	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
Pamieć FLASH (pendrive)	Pożar (naturalne)	1.8	TAK
Pamieć FLASH (pendrive)	Pożar (przypadkowe)	1.8	TAK
Windows	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.8	TAK
Sieć LAN	Pożar (naturalne)	1.8	TAK
Router	Nieprawidłowa konserwacja sprzętu (przypadkowe)	1.8	TAK
Przełącznik (switch)	Nieprawidłowa konserwacja sprzętu (przypadkowe)	1.8	TAK
Dane osobowe na dysku twardym	Błąd monitorowania (przypadkowe)	1.7	TAK
Dane osobowe na przenośnym nośniku pamięci	Błąd monitorowania (przypadkowe)	1.7	TAK
Laptop	Kradzież nośników (umyślne)	1.7	TAK
Laptop	Przerwy w łączności, transmisji danych (umyślne)	1.7	TAK
Komputer PC	Kradzież nośników (umyślne)	1.7	TAK

DOSTEPNOŚĆ			
AKTYWA	**ZAGROŻENIA**	**RYZYKO**	**AKC**
Drukarka	Sfałszowanie oprogramowania (przypadkowe)	1.7	TAK

INTEGRALNOŚĆ			
AKTYWA	**ZAGROŻENIA**	**RYZYKO**	**AKC**
Dysk twardy	Zmiana informacji (umyślne)	3.5	TAK
Dane osobowe na przenośnym nośniku pamięci	Złośliwe oprogramowanie (umyślne)	3.2	TAK
Pamieć FLASH (pendrive)	Zmiana informacji (umyślne)	3.2	TAK
Hosting danych osobowych	Zmiana informacji (umyślne)	3.1	TAK
Drukarka	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	2.7	TAK
Router	Złośliwe oprogramowanie (umyślne)	2.7	TAK
Przełącznik (switch)	Złośliwe oprogramowanie (umyślne)	2.7	TAK
Dane osobowe na dysku twardym	Zmiana informacji (umyślne)	2.6	TAK
Dane osobowe na przenośnym nośniku pamięci	Zmiana informacji (umyślne)	2.6	TAK
Pakiet biurowy office	Zmiana informacji (umyślne)	2.5	TAK
Klient e-mail	Zmiana informacji (umyślne)	2.5	TAK
Oprogramowanie księgowe	Zmiana informacji (umyślne)	2.5	TAK
Oprogramowanie do zarządzania personelem	Zmiana informacji (umyślne)	2.5	TAK
Laptop	Złośliwe oprogramowanie (umyślne)	2.4	TAK
Komputer PC	Złośliwe oprogramowanie (umyślne)	2.4	TAK
Pakiet biurowy office	Złośliwe oprogramowanie (umyślne)	2.4	TAK
Klient e-mail	Złośliwe oprogramowanie (umyślne)	2.4	TAK
Oprogramowanie księgowe	Złośliwe oprogramowanie (umyślne)	2.4	TAK
Oprogramowanie do zarządzania personelem	Złośliwe oprogramowanie (umyślne)	2.4	TAK
Dane osobowe na dysku twardym	Złośliwe oprogramowanie (umyślne)	2.3	TAK
Pliki danych	Zmiana informacji (umyślne)	2.3	TAK
Windows	Złośliwe oprogramowanie (umyślne)	2.3	TAK
Windows	Zmiana informacji (umyślne)	2.3	TAK
Pliki danych	Złośliwe oprogramowanie (umyślne)	2.2	TAK
Internet	Zmiana informacji (umyślne)	2.2	TAK
Internet	Złośliwe oprogramowanie (umyślne)	2.1	TAK
Hosting danych osobowych	Manipulacja konfiguracją (umyślne)	1.9	TAK
Drukarka	Sfałszowanie oprogramowania (umyślne)	1.9	TAK
Drukarka	Błąd monitorowania (przypadkowe)	1.8	TAK
Dane osobowe w postaci wydruków na papierze	Błąd użytkowania (przypadkowy)	1.7	TAK
Laptop	Zmiana informacji (umyślne)	1.7	TAK
Komputer PC	Zmiana informacji (umyślne)	1.7	TAK
Wydruki papierowe	Błąd użytkowania (przypadkowy)	1.7	TAK
Dane osobowe w postaci wydruków na papierze	Błąd administrowania (przypadkowe)	1.5	TAK
Wydruki papierowe	Błąd administrowania (przypadkowe)	1.5	TAK
Dane osobowe na dysku twardym	Błąd monitorowania (przypadkowe)	1.4	TAK
Dane osobowe na przenośnym nośniku pamięci	Błąd monitorowania (przypadkowe)	1.4	TAK
Dane osobowe na przenośnym nośniku pamięci	Sfałszowanie oprogramowania (umyślne)	1.4	TAK
Dane osobowe w postaci wydruków na papierze	Nieautoryzowany dostęp (umyślne)	1.4	TAK
Hosting danych osobowych	Nieautoryzowany dostęp (umyślne)	1.4	TAK
Pamieć FLASH (pendrive)	Nieautoryzowany dostęp (umyślne)	1.4	TAK
Wydruki papierowe	Nieautoryzowany dostęp (umyślne)	1.4	TAK

INTEGRALNOŚĆ			
AKTYWA	**ZAGROŻENIA**	**RYZYKO**	**AKC**
Pliki danych	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.3	TAK
Laptop	Błąd monitorowania (przypadkowe)	1.3	TAK
Laptop	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	1.3	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 księgowe	Błąd monitorowania (przypadkowe)	1.3	TAK
Oprogramowanie do zarządzania personelem	Błąd monitorowania (przypadkowe)	1.3	TAK
Sieć LAN	Błąd monitorowania (przypadkowe)	1.3	TAK
Router	Błąd monitorowania (przypadkowe)	1.3	TAK
Przełącznik (switch)	Błąd monitorowania (przypadkowe)	1.3	TAK
Pliki danych	Nieautoryzowany dostęp (umyślne)	1.1	TAK
Drukarka	Sfałszowanie oprogramowania (przypadkowe)	1.1	TAK
Router	Błąd administrowania (przypadkowe)	1.1	TAK
Przełącznik (switch)	Błąd administrowania (przypadkowe)	1.1	TAK
Dane osobowe na przenośnym nośniku pamięci	Błąd użytkowania (przypadkowy)	1.0	TAK
Dane osobowe na przenośnym nośniku pamięci	Błąd administrowania (przypadkowe)	1.0	TAK
Drukarka	Błąd użytkowania (przypadkowy)	1.0	TAK
Drukarka	Błąd administrowania (przypadkowe)	1.0	TAK
Windows	Błąd administrowania (przypadkowe)	1.0	TAK
Pakiet biurowy office	Błąd użytkowania (przypadkowy)	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
Dysk twardy	Nieautoryzowany dostęp (umyślne)	0.9	TAK
Pakiet biurowy office	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.9	TAK
Klient e-mail	Błąd monitorowania (przypadkowe)	0.9	TAK
Klient e-mail	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.9	TAK
Oprogramowanie księgowe	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.9	TAK
Oprogramowanie do zarządzania personelem	Użycie nielegalnego lub skopiowanego oprogramowania (umyślne)	0.9	TAK
WIFI	Błąd monitorowania (przypadkowe)	0.9	TAK
Dostęp do internetu świadczony przez operatora zewnętrznego	Błąd monitorowania (przypadkowe)	0.9	TAK
Laptop	Nieautoryzowany dostęp (umyślne)	0.8	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 księgowe	Nieautoryzowany dostęp (umyślne)	0.8	TAK
Oprogramowanie do zarządzania personelem	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

INTEGRALNOŚĆ			
AKTYWA	**ZAGROŻENIA**	**RYZYKO**	**AKC**
Dane osobowe na przenośnym nośniku pamięci	Sfałszowanie oprogramowania (przypadkowe)	0.7	TAK
Pliki danych	Sfałszowanie oprogramowania (przypadkowe)	0.7	TAK
Laptop	Błąd administrowania (przypadkowe)	0.7	TAK
Laptop	Sfałszowanie oprogramowania (przypadkowe)	0.7	TAK
Laptop	Sfałszowanie oprogramowania (umyślne)	0.7	TAK
Komputer PC	Błąd administrowania (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
Drukarka	Nieautoryzowany dostęp (umyślne)	0.7	TAK
Windows	Manipulacja konfiguracją (umyślne)	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	Manipulacja konfiguracją (umyślne)	0.7	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.