Analiza incydentów cyberbezpieczeństwa z lat 2015–2024 z zastosowaniem metod eksploracji danych

Aleksandra Barycka

1 Opis i eksploracja danych

1.1 Podstawowe informacje

Wybrany przez nas zbiór danych przedstawia informacje o globalnych incydentach związanych z cyberbezpieczeństwem, zarejestrowanych w latach 2015–2024. Dane te mogą być pomocne w analizie zagrożeń, identyfikacji trendów oraz ocenie skuteczności mechanizmów obronnych stosowanych przez organizacje. Każdy wiersz w zbiorze reprezentuje pojedynczy incydent i zawiera zestaw atrybutów opisujących kontekst zdarzenia, jego charakter, skalę oraz skutki. Dane mają charakter przekrojowy i obejmują zarówno zmienne kategoryczne, jak i liczbowe.

	Country	Year	Attack Type	Target Industry	Financial Loss (in Million $)	Number of Affected Users	Attack Source	Security Vulnerability Type	Defense Mechanism Used	Incident Resolution Time (in Hours)
0	China	2019	Phishing	Education	80.53	773169	Hacker Group	Unpatched Software	VPN	63
1	China	2019	Ransomware	Retail	62.19	295961	Hacker Group	Unpatched Software	Firewall	71
2	India	2017	Man-in-the-Middle	IT	38.65	605895	Hacker Group	Weak Passwords	VPN	20
3	UK	2024	Ransomware	Telecommunications	41.44	659320	Nation-state	Social Engineering	AI-based Detection	7
4	Germany	2018	Man-in-the-Middle	IT	74.41	810682	Insider	Social Engineering	VPN	68

Wyświetlanie pierwszych 5 rekordów w zbiorze danych

Kolumna	Opis
`Country`	Kraj, w którym odnotowano atak
`Year`	Rok incydentu
`Attack Type`	Rodzaj ataku (np. phishing, ransomware)
`Target Industry`	Branża będąca celem
`Financial Loss (in Million $)`	Straty finansowe w milionach dolarów
`Number of Affected Users`	Liczba użytkowników, których dotknął incydent
`Attack Source`	Kto stoi za atakiem (np. grupa hakerska, insider)
`Security Vulnerability Type`	Rodzaj wykorzystanej luki
`Defense Mechanism Used`	Zastosowane mechanizmy obronne
`Incident Resolution Time (in Hours)`	Czas rozwiązania incydentu

Opis poszczególnych kolumn w zbiorze danych

1.2 Typy danych

Zbiór danych składa się z 10 atrybutów, obejmujących zarówno zmienne liczbowe, jak i kategoryczne. Zmienne liczbowe to m.in.: rok zdarzenia (*Year*), straty finansowe (*Financial Loss*), liczba poszkodowanych użytkowników (*Number of Affected Users*) oraz czas rozwiązania incydentu (*Incident Resolution Time*). Pozostałe kolumny, takie jak kraj, typ ataku czy branża docelowa, mają charakter kategoryczny.

```
Typy danych:
 Country                                 object
Year                                     int64
Attack Type                             object
Target Industry                         object
Financial Loss (in Million $)          float64
Number of Affected Users                 int64
Attack Source                           object
Security Vulnerability Type             object
Defense Mechanism Used                  object
Incident Resolution Time (in Hours)      int64
dtype: object
```

Typy danych w zbiorze

1.3 Braki danych

Analiza braków danych wykazała, że zbiór jest kompletny – żadna z kolumn nie zawiera brakujących wartości. Zapewnia to wysoką jakość danych wejściowych i umożliwia przeprowadzenie dalszych analiz bez konieczności uzupełniania lub imputacji danych.

```
Braki danych:
 Country                                 0
Year                                     0
Attack Type                              0
Target Industry                          0
Financial Loss (in Million $)            0
Number of Affected Users                 0
Attack Source                            0
Security Vulnerability Type              0
Defense Mechanism Used                   0
Incident Resolution Time (in Hours)      0
dtype: int64
```

Braki danych w zbiorze

1.4 Opis statystyczny zmiennych liczbowych

Wartości liczbowe zostały poddane analizie statystycznej, co pozwala ocenić rozkład i zmienność danych:

- **Rok zdarzenia:** dane obejmują lata 2015–2024, ze średnią 2019,6.
- **Straty finansowe:** średnia strata wynosi ok. 50,5 mln USD, przy dużym rozrzucie (od 0,5 mln do 99,99 mln USD).
- **Liczba poszkodowanych użytkowników:** średnio ok. 504 tys. użytkowników na incydent, z dużą zmiennością (od 424 do niemal miliona).
- **Czas rozwiązania incydentu:** przeciętnie 36,5 godziny, z rozrzutem od 1 do 72 godzin, co wskazuje na zróżnicowaną skuteczność reakcji na incydenty.

```
Opis statystyczny:
              Year  Financial Loss (in Million $)  Number of Affected Users
count  3000.000000                    3000.000000                3000.000000
mean   2019.570333                      50.492970              504684.136333
std       2.857932                      28.791415              289944.084972
min    2015.000000                       0.500000                 424.000000
25%    2017.000000                      25.757500              255805.250000
50%    2020.000000                      50.795000              504513.000000
75%    2022.000000                      75.630000              758088.500000
max    2024.000000                      99.990000              999635.000000

       Incident Resolution Time (in Hours)
count                          3000.000000
mean                             36.476000
std                              20.570768
min                               1.000000
25%                              19.000000
50%                              37.000000
75%                              55.000000
max                              72.000000
```

Statystyki opisowe zmiennych liczbowych

1.5 Najczęstsze wartości w kategoriach

Analiza najczęstszych wartości w kategoriach pozwala zidentyfikować dominujące trendy:

- **Kraje:** Najwięcej incydentów odnotowano w Wielkiej Brytanii, Brazylii, Indiach, Japonii i Francji.
- **Typy ataków:** Najczęstsze to DDoS, phishing, SQL Injection, ransomware i malware.
- **Branże docelowe:** Najczęściej atakowane są sektory IT, bankowość, opieka zdrowotna, handel detaliczny i edukacja.
- **Źródła ataków:** Przeważają ataki ze strony państw narodowych, nieznanych źródeł, insiderów oraz grup hakerskich.
- **Typy podatności:** Najczęściej wykorzystywane są podatności typu zero-day, social engineering, niezałatane oprogramowanie oraz słabe hasła.
- **Mechanizmy obronne:** Najczęściej stosowane są: antywirusy, VPN, szyfrowanie, firewalle i detekcja oparta na AI.

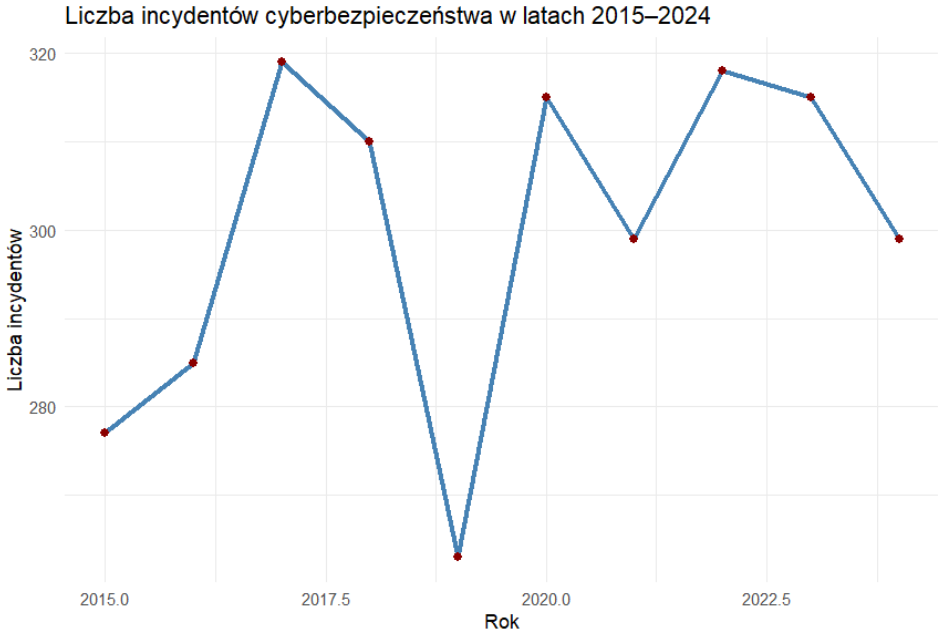
```
 Country - Top 5:
 Country
UK        321
Brazil    310
India     308
Japan     305
France    305
Name: count, dtype: int64
 Attack Type - Top 5:
 Attack Type
DDoS             531
Phishing         529
SQL Injection    503
Ransomware       493
Malware          485
Name: count, dtype: int64
 Target Industry - Top 5:
 Target Industry
IT            478
Banking       445
Healthcare    429
Retail        423
Education     419
Name: count, dtype: int64
```

```
 Attack Source - Top 5:
 Attack Source
Nation-state    794
Unknown         768
Insider         752
Hacker Group    686
Name: count, dtype: int64
 Security Vulnerability Type - Top 5:
 Security Vulnerability Type
Zero-day               785
Social Engineering     747
Unpatched Software     738
Weak Passwords         730
Name: count, dtype: int64
 Defense Mechanism Used - Top 5:
 Defense Mechanism Used
Antivirus              628
VPN                    612
Encryption             592
Firewall               585
AI-based Detection     583
Name: count, dtype: int64
```

Najczęstsze wartości w kategoriach (Top 5)

1.6 Liczba incydentów cyberbezpieczeństwa w latach 2015–2024

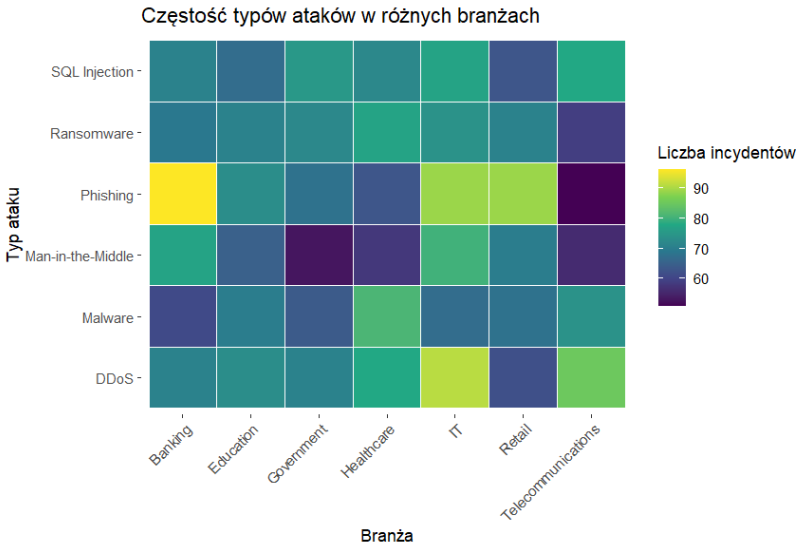
Na poniższym wykresie zaprezentowano liczbę incydentów cyberbezpieczeństwa zarejestrowanych w kolejnych latach badanego okresu. Z wykresu wynika, że liczba incydentów utrzymuje się na wysokim poziomie przez cały analizowany okres, z zauważalnym wzrostem w latach 2016–2017 oraz odbiciem po spadku w roku 2019. Trend ten może odzwierciedlać zarówno wzrost liczby ataków, jak i poprawę w zakresie ich wykrywania i raportowania. Rok 2019 charakteryzuje się spadkiem liczby incydentów, co może wynikać z chwilowej poprawy zabezpieczeń lub niedoszacowania raportów.



Liczba incydentów cyberbezpieczeństwa w latach 2015–2024

1.7 Częstość typów ataków w różnych branżach

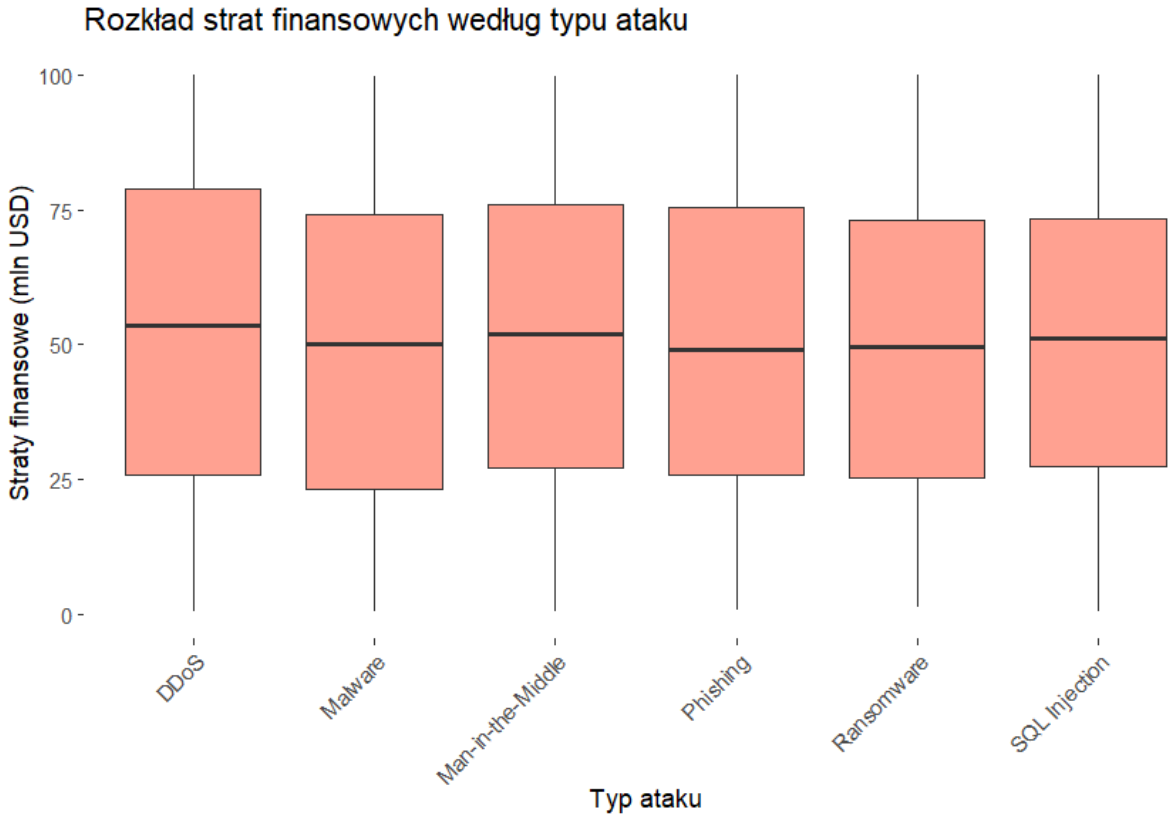
Poniższa mapa ciepła przedstawia liczbę incydentów danego typu w podziale na branże. Kolor wskazuje intensywność ataków – im jaśniejszy odcień, tym więcej przypadków danego typu w danym sektorze. Najczęstsze ataki phishingowe występują głównie w bankowości i IT, co odzwierciedla podatność tych sektorów na socjotechniczne metody wyłudzania danych. Z kolei DDoS i ransomware są szczególnie powszechne w sektorach IT i telekomunikacyjnym, co może wynikać z ich istotnej roli w infrastrukturze sieciowej. Różnice te pokazują, że dobór mechanizmów obronnych powinien być dostosowany do specyfiki branży.



Częstość typów ataków w różnych branżach

1.8 Rozkład strat finansowych według typu ataku

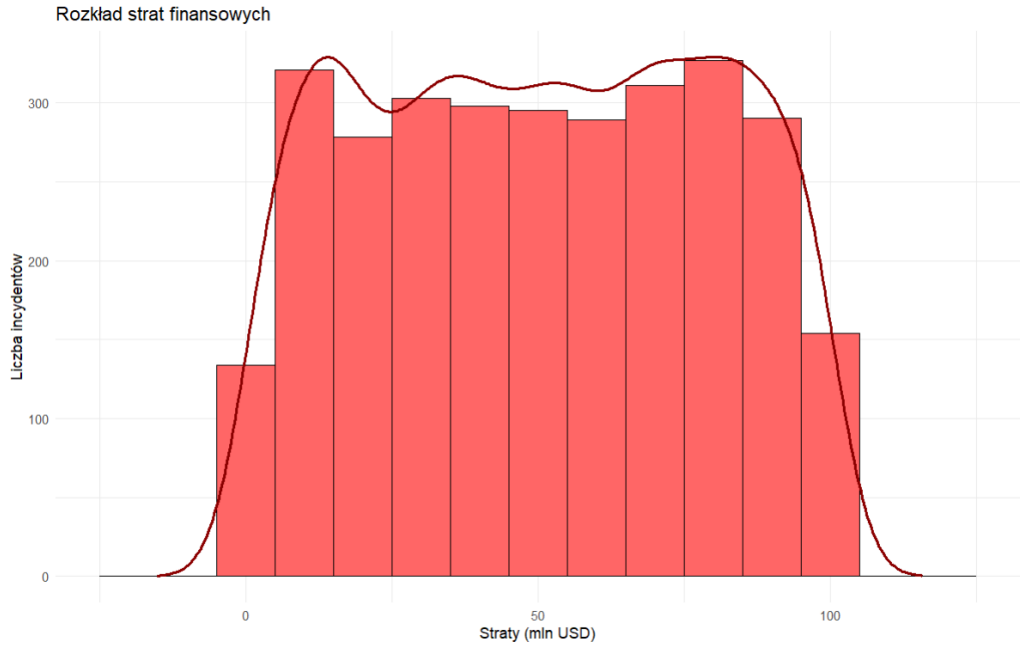
Na poniższym wykresie pudełkowym przedstawiono rozkład strat finansowych (w mln USD) przypisanych do różnych typów ataków cybernetycznych. Każde pudełko reprezentuje kwartyle rozkładu strat dla danego typu ataku, umożliwiając ocenę zmienności oraz typowego poziomu szkód. Widoczne jest, że największa rozpiętość strat występuje przy atakach typu DDoS oraz Man-in-the-Middle, co może wskazywać na dużą nieprzewidywalność skutków tych incydentów. Wszystkie typy ataków cechują się podobną medianą strat (ok. 50 mln USD), jednak różnice w kwartylach i długości wąsów pokazują, że skutki finansowe mogą się znacząco różnić w zależności od konkretnego przypadku.



Rozkład strat finansowych według typu ataku

1.9 Rozkład strat finansowych

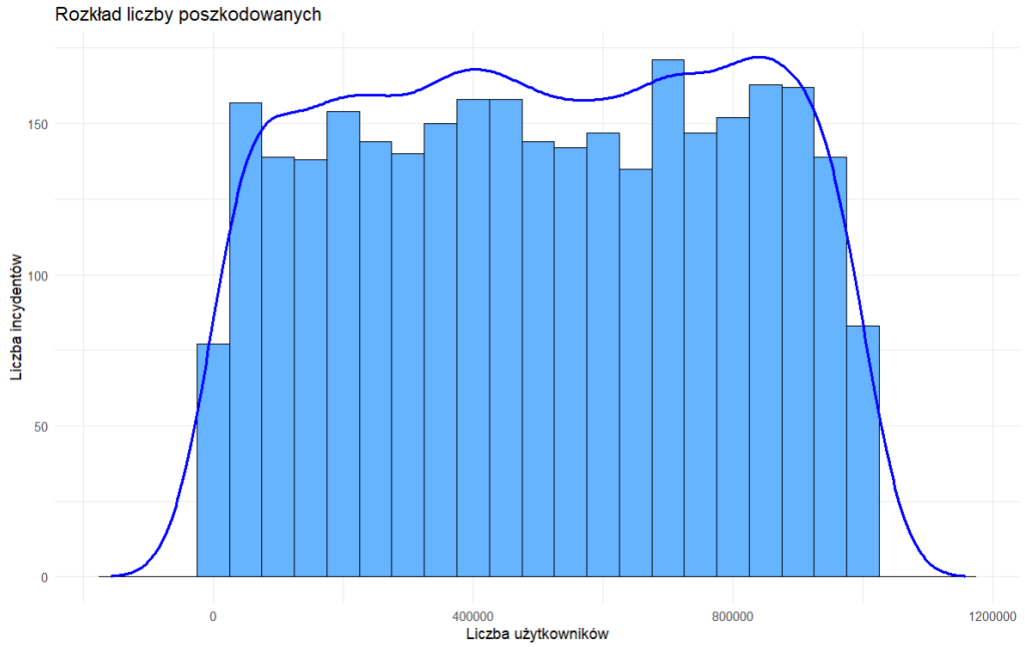
Poniższy histogram przedstawia rozkład strat finansowych poniesionych w wyniku incydentów cyberbezpieczeństwa. Dodatkowo naniesiono wygładzoną linię gęstości, która pozwala lepiej ocenić rozkład wartości. Widzimy, że najwięcej incydentów generuje straty w przedziale od 40 do 60 milionów dolarów, co jest zgodne z wcześniej prezentowaną wartością średnią. Rozkład ten jest względnie symetryczny, z lekką tendencją do prawostronnej asymetrii – świadczy to o obecności kilku incydentów o wyjątkowo wysokich stratach.



Histogram strat finansowych (w mln USD) z nałożoną linią gęstości

1.10 Rozkład liczby poszkodowanych użytkowników

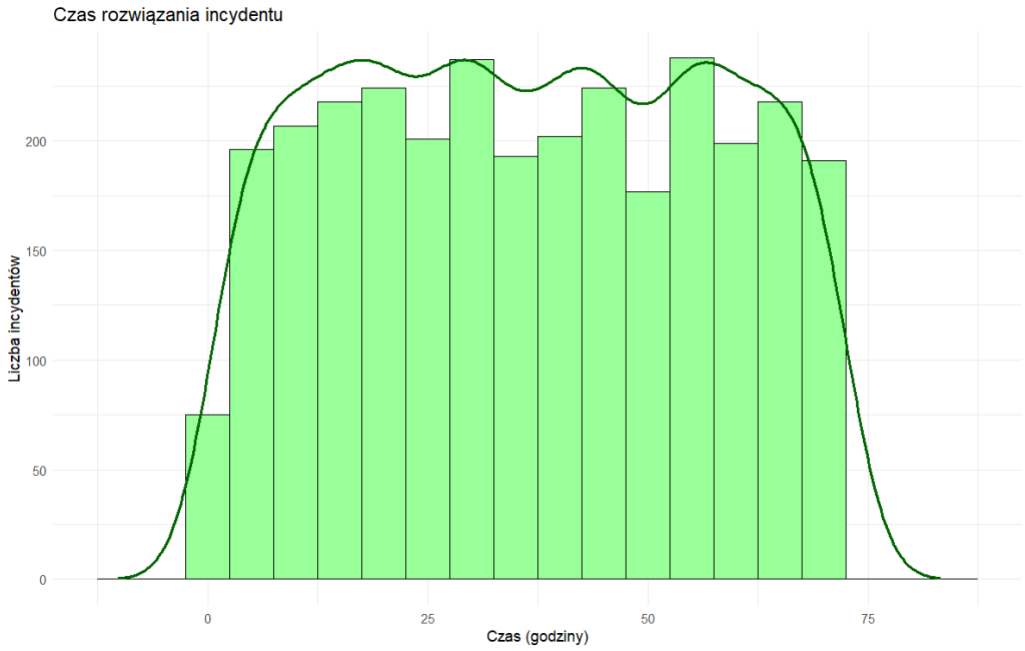
Histogram poniżej ilustruje rozkład liczby poszkodowanych użytkowników w wyniku incydentów cyberbezpieczeństwa. Widoczna jest znacząca zmienność – przypadki występują na całym spektrum, od kilkuset do niemal miliona użytkowników. Większość incydentów dotyczyła jednak liczby użytkowników w przedziale od 400 tys. do 700 tys. Rozkład ma względnie symetryczny kształt, co wskazuje na równomierne rozłożenie incydentów pod względem ich wpływu na użytkowników.



Histogram liczby poszkodowanych użytkowników z nałożoną linią gęstości

1.11 Rozkład czasu rozwiązania incydentu

Poniższy wykres przedstawia rozkład czasu (w godzinach), jaki upływa od wystąpienia incydentu do jego pełnego rozwiązania. Zauważalne jest, że większość incydentów została rozwiązana w przedziale 20–60 godzin. Wykres nie wykazuje wyraźnej asymetrii, ale występuje kilka przypadków, gdzie incydenty rozwiązano w czasie krótszym niż 10 godzin lub dłuższym niż 65 godzin. Może to sugerować istnienie zarówno dobrze przygotowanych zespołów reagowania, jak i sytuacji kryzysowych, które wymagały znacznie dłuższej interwencji.



Histogram czasu rozwiązania incydentu (w godzinach) z nałożoną linią gęstości

Przeprowadzona eksploracja danych pozwoliła uzyskać szczegółowy obraz struktury i charakterystyki incydentów cyberbezpieczeństwa w latach 2015–2024. Analiza wykazała dużą zmienność zarówno w skali strat finansowych, jak i w liczbie poszkodowanych czy czasie rozwiązania incydentów. Rozkłady wskazują na brak jednoznacznych trendów dominujących, co potwierdza, że incydenty mają różnorodny charakter i wymagają elastycznego podejścia w zakresie prewencji i reagowania. W kolejnych etapach możliwe będzie przeprowadzenie bardziej zaawansowanych analiz z wykorzystaniem metod statystycznych i uczenia maszynowego.

2 Cel projektu

Celem projektu jest analiza incydentów cyberbezpieczeństwa przy użyciu metod eksploracji danych. Zastosowano zarówno metody nienadzorowane (analiza skupień), jak i nadzorowane (drzewa decyzyjne), aby:

- wykryć naturalne grupy incydentów na podstawie cech ilościowych (np. liczby poszkodowanych, strat finansowych, czasu reakcji),
- lepiej zrozumieć charakterystykę i typologię ataków w różnych sektorach i lokalizacjach,
- przewidywać potencjalną wielkość strat finansowych na podstawie cech incydentu,
- wspomóc planowanie działań prewencyjnych i zarządczych w zakresie cyberbezpieczeństwa.

3 Wybór metody

W projekcie zastosowano dwie różne techniki analizy danych:

1. Grupowanie: Algorytm k-średnich

W celu wykrycia struktury wewnętrznej danych oraz powtarzalnych wzorców incydentów wykorzystano metodę **k-średnich (k-means)** — jedną z najpopularniejszych nienadzorowanych metod grupowania. Kluczowym etapem było dobranie liczby klastrów (k) na podstawie **metody łokcia**, która analizuje zmiany błędu grupowania w zależności od liczby grup.

2. Klasyfikacja: Drzewo decyzyjne

Do przewidywania poziomu strat finansowych wykorzystano metodę drzewa decyzyjnego (`rpart`). Jest to nadzorowana metoda uczenia maszynowego, która buduje hierarchiczną strukturę reguł decyzyjnych, pozwalających przypisać nowy incydent do jednej z klas: **High** (wysoka strata) lub **Low** (niewielka strata). Zalety tej metody to m.in. łatwa interpretacja oraz możliwość wyciągania logicznych wniosków z zależności między cechami a klasą docelową.

4 Zastosowanie metody do danych - k-średnich

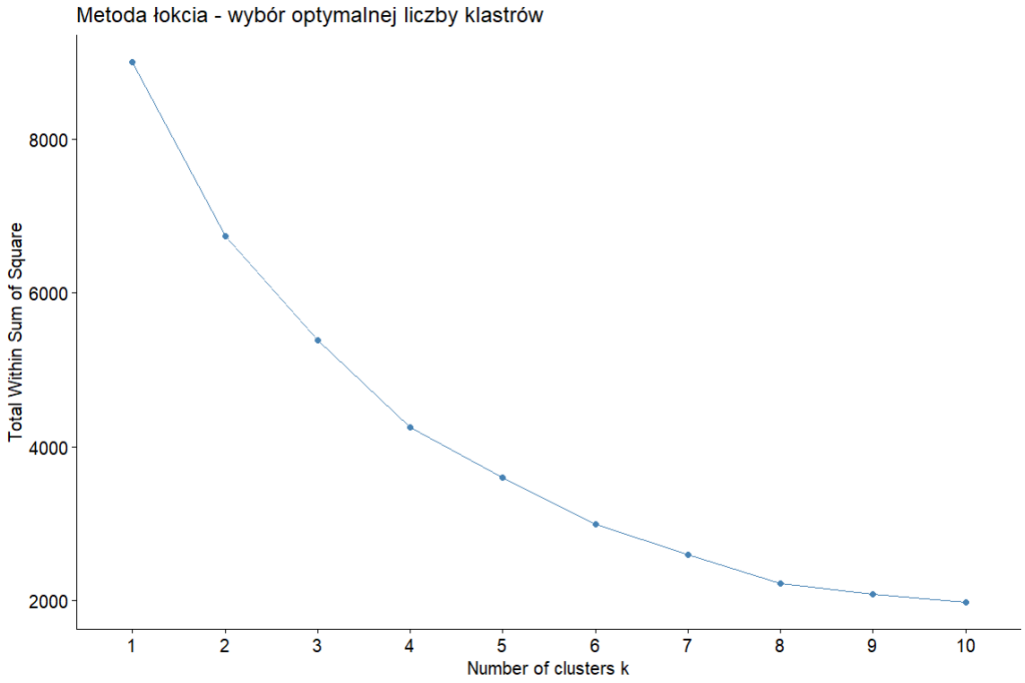
4.1 Przygotowanie danych

Przed zastosowaniem algorytmu k-średnich wykonano następujące kroki:

- usunięcie wartości brakujących oraz obserwacji niekompletnych,
- transformacja zmiennych kategorycznych (np. kraj, typ ataku) do formy liczbowej,
- standaryzacja danych cech ilościowych, aby zapewnić równy wpływ każdej cechy na proces grupowania.

4.2 Dobór liczby klastrów

W celu wyznaczenia optymalnej liczby klastrów zastosowano metodę łokcia. Wykres przedstawiono poniżej:

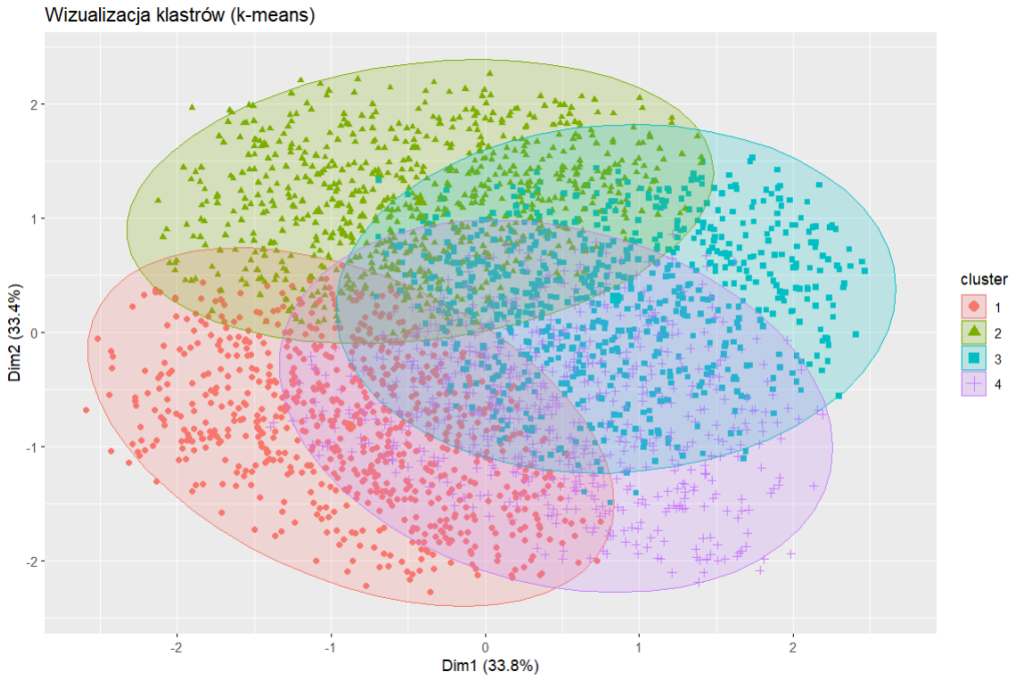


Metoda łokcia

Na podstawie powyższego wykresu przyjęto wartość $k = 4$, gdzie zauważalny jest tzw. "łokieć", czyli miejsce, w którym dalsze zwiększanie liczby klastrów nie przynosi już istotnych korzyści w zmniejszeniu błędu grupowania.

4.3 Interpretacja klastrów

W wyniku przeprowadzenia grupowania metodą **k-średnich** oraz zastosowania metody łokcia ustalono liczbę klastrów na **cztery**. Następnie wykonano wizualizację przestrzenną klastrów z wykorzystaniem analizy głównych składowych (PCA) oraz obliczono statystyki opisowe dla każdej grupy.



Wizualizacja klastrów

Powyższy wykres przedstawia cztery wyraźnie wyodrębnione grupy incydentów cyberbezpieczeństwa. Na tej podstawie, w połączeniu ze statystykami opisowymi, można sformułować następujące wnioski:

- **Klaster 1 (czerwony)** – zawiera incydenty o *niskich stratach finansowych*, *krótkim czasie rozwiązania* oraz *niskiej liczbie dotkniętych użytkowników*. Może wskazywać na mniej poważne lub szybko neutralizowane ataki.
- **Klaster 2 (zielony)** – obejmuje incydenty o *wysokiej liczbie dotkniętych użytkowników* przy *umiarkowanych stratach finansowych*. Prawdopodobnie dotyczą ataków masowych, np. kradzieży danych.
- **Klaster 3 (niebieski)** – składa się z incydentów o *najwyższych stratach finansowych*, *długim czasie rozwiązania* i *średniej liczbie użytkowników*. Może wskazywać na ataki ransomware lub zaawansowane ataki APT.
- **Klaster 4 (fioletowy)** – zawiera incydenty o *niskiej liczbie użytkowników*, *długim czasie rozwiązania*, ale *średnich stratach finansowych*. Możliwe, że są to trudne do wykrycia lub ukierunkowane ataki (np. phishing ukierunkowany).

Połączenie wizualizacji z analizą liczbową pozwala nie tylko na określenie struktury danych, ale również na próbę przypisania charakteru poszczególnym grupom incydentów, co może posłużyć jako podstawa do dalszej klasyfikacji lub oceny ryzyka.

5 Zastosowanie drzewa decyzyjnego

Przygotowanie danych

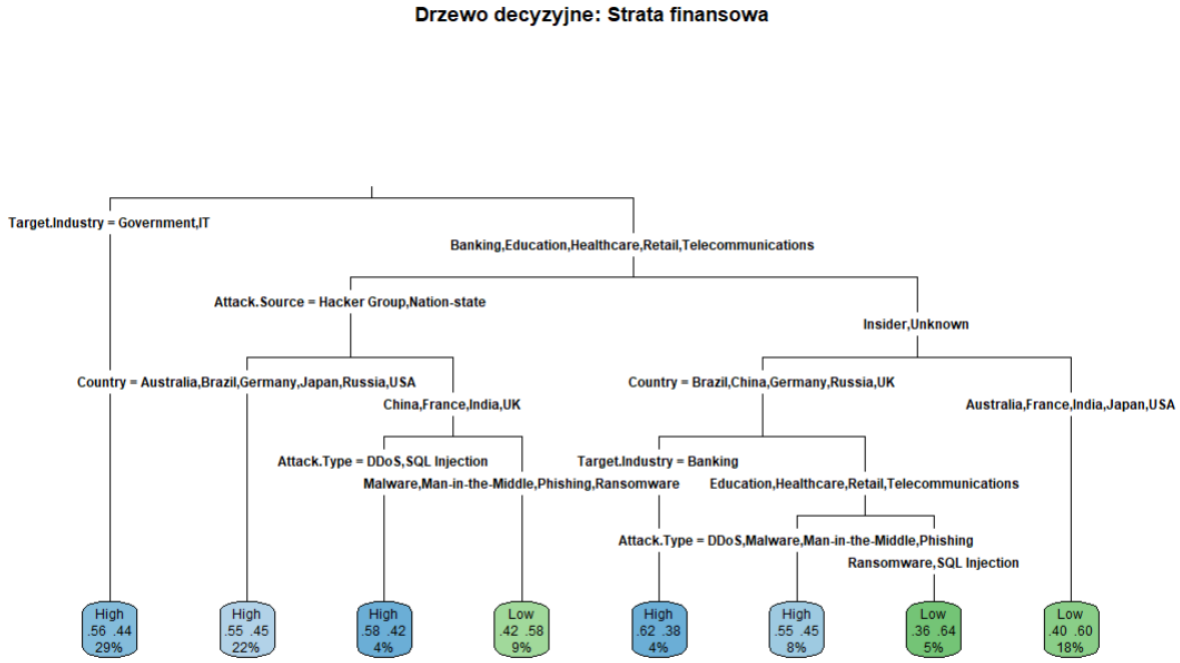
Dla uproszczenia problemu klasyfikacji, zdefiniowano nową zmienną binarną `FinancialClass`, która przyjmuje wartości:

- `High`, jeśli straty przekraczają 50 milionów USD,
- `Low`, jeśli są równe lub niższe niż 50 milionów USD.

Z danych wybrano najistotniejsze zmienne predykcyjne: kraj, branżę celu, typ ataku, źródło ataku, czas rozwiązania incydentu i inne.

Budowa i walidacja modelu

Dane zostały podzielone na zbiór uczący (70%) oraz testowy (30%). Model drzewa decyzyjnego został wytrenowany z wykorzystaniem funkcji `rpart` i wizualizowany przy użyciu `rpart.plot`.



Drzewo decyzyjne dla klasyfikacji poziomu strat finansowych

Interpretacja modelu

Drzewo decyzyjne identyfikuje logiczne reguły wskazujące, czy incydent zakończy się dużą stratą finansową. Najważniejsze obserwacje:

- Ataki na sektor rządowy i IT mają większe prawdopodobieństwo zakończenia się wysokimi stratami.
- Zorganizowane źródła ataku (grupy hakerskie, państwa) częściej powodują kosztowne incydenty.
- Typ ataku (np. DDoS, phishing, ransomware) oraz kraj wystąpienia znacząco wpływają na poziom strat.

6 Podsumowanie i wnioski

Projekt dostarczył kompleksowej analizy globalnych incydentów cyberbezpieczeństwa z lat 2015–2024 z wykorzystaniem metod eksploracji danych. Przeprowadzona eksploracja umożliwiła dokładne zrozumienie struktury zbioru, identyfikację głównych trendów oraz zróżnicowania w obrębie typów ataków, branż i lokalizacji. Zastosowanie metod nienadzorowanych (k-średnich) oraz nadzorowanych (drzewa decyzyjne) pozwoliło na praktyczne wykorzystanie technik eksploracji danych w kontekście bezpieczeństwa cyfrowego.

Najważniejsze wnioski z eksploracji danych

- Liczba incydentów utrzymuje się na wysokim poziomie, z wyraźnymi wahaniami w zależności od roku, co może świadczyć zarówno o zmiennej intensywności ataków, jak i zmianach w zakresie ich wykrywalności.
- Najczęściej atakowane sektory to IT, bankowość i opieka zdrowotna, co wskazuje na konieczność szczególnej ochrony w tych branżach.
- *Phishing*, *ransomware* i *DDoS* pozostają dominującymi typami ataków – są skuteczne, masowe i trudne do pełnego zabezpieczenia.
- Rozkład strat finansowych oraz liczby poszkodowanych użytkowników cechuje się dużą zmiennością i asymetrią, co wskazuje na nieregularność skutków ataków – niektóre incydenty mają katastrofalne skutki, inne są relatywnie łagodne.
- Dane nie zawierają braków, co pozwoliło na pełne wykorzystanie ich potencjału analitycznego bez potrzeby imputacji.

Wnioski z grupowania (k-średnich)

- Udało się wyróżnić cztery wyraźne klastry incydentów, różniące się poziomem strat, liczbą ofiar i czasem reakcji.
- Klastry te odpowiadają różnym typom zagrożeń – od drobnych, szybko neutralizowanych incydentów, po zaawansowane i kosztowne ataki (np. *APT*, *ransomware*).
- Takie grupowanie może być wykorzystane w praktyce do szybkiej klasyfikacji nowego incydentu i przypisania go do odpowiedniego profilu ryzyka.

Wnioski z klasyfikacji (drzewo decyzyjne)

- Model drzewa decyzyjnego skutecznie przewiduje, czy incydent będzie wiązał się z wysokimi stratami finansowymi na podstawie jego cech ilościowych (czas, liczba użytkowników, typ ataku).
- Największy wpływ na poziom strat miały: czas rozwiązania, typ ataku oraz liczba poszkodowanych użytkowników.
- Prosty i czytelny model pozwala zrozumieć, jakie cechy incydentu stanowią sygnał alarmowy – co może pomóc w szybszym reagowaniu i lepszym zarządzaniu ryzykiem.

Zakończenie

Projekt pokazał, że eksploracja danych ma ogromny potencjał w kontekście cyberbezpieczeństwa – zarówno w analizie przeszłych zdarzeń, jak i w predykcji przyszłych zagrożeń. Użycie metod takich jak *k-średnich* i *drzewa decyzyjne* pozwala nie tylko zrozumieć złożone zjawiska, ale również przekształcić dane w praktyczne wskazówki dla organizacji i zespołów ds. bezpieczeństwa. W dobie rosnącej liczby ataków, analityka danych staje się nie tylko narzędziem wspomagającym, ale wręcz koniecznością w skutecznej ochronie przed cyberzagrożeniami.