Co zrobić po incydencie?

Czym jest incydent bezpieczeństwa?

- Incydent bezpieczeństwa informacji to zdarzenie, które doprowadziło lub mogło doprowadzić do naruszenia czy utraty poufności danych, integralności systemów i ciągłości procesów biznesowych

- Do listy incydentów bezpieczeństwa informacji zaliczane są infekcje firmowej sieci lub komputerów złośliwym oprogramowaniem, ataki socjotechniczne (np. phishing) i kradzież fizycznych nośników danych.

Szybka reakcja na incydent bezpieczeństwa jest kluczowa z kilku powodów:

- Minimalizacja szkód:
- Ograniczenie rozprzestrzeniania się incydentu:
- Skrócenie czasu przestoju:
- Ochrona reputacji:
- Spełnienie wymagań prawnych:

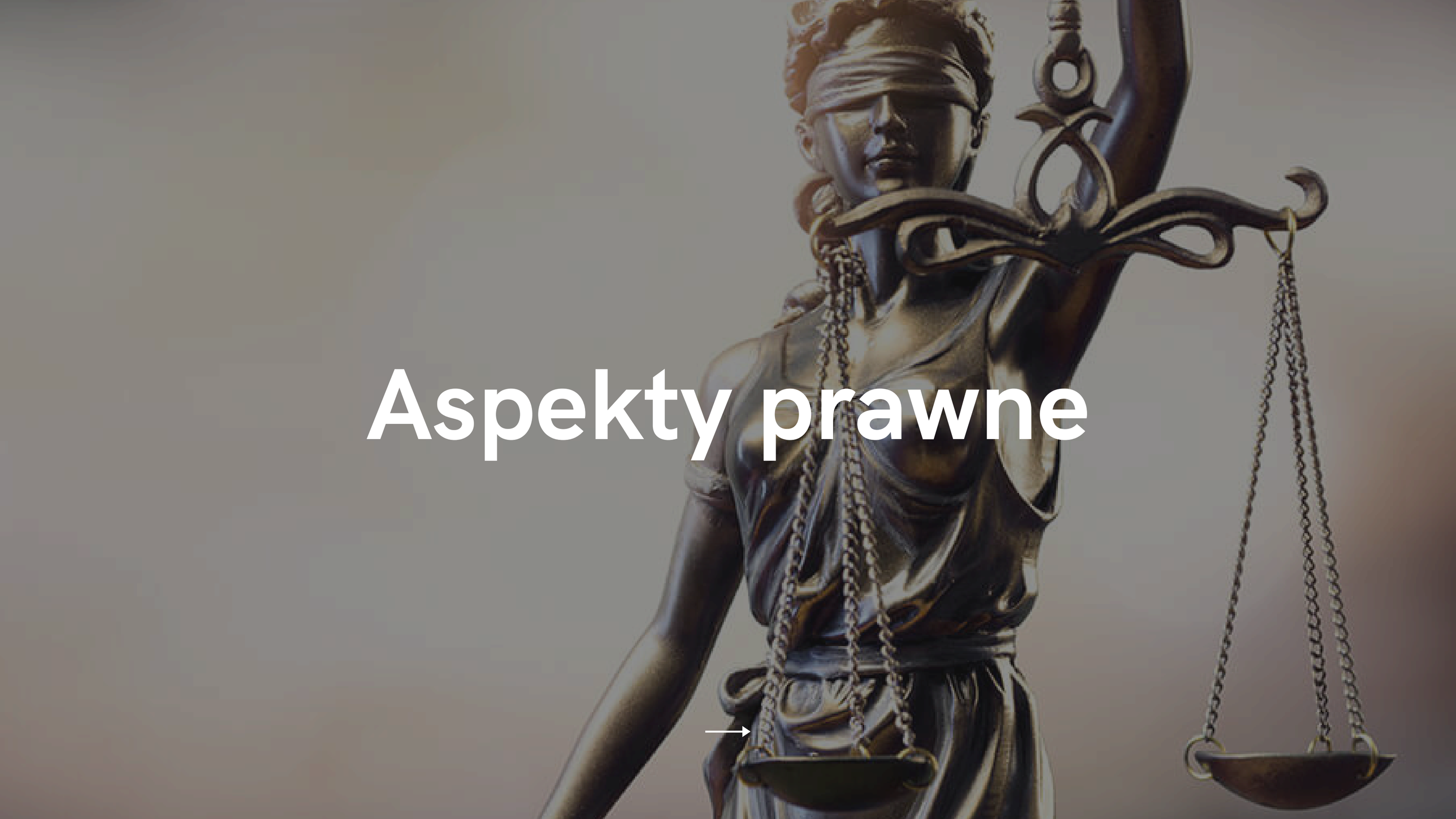
→

Korzyści z właściwego zarządzania incydentami bezpieczeństwa

- Zwiększenie bezpieczeństwa systemu
- Poprawa procesu reagowania
- Oszczędności finansowe
- Zgodność z przepisami i regulacjami
- Zwiększenie zaufania interesariuszy
- Udoskonalenie monitoringu i wykrywania

→

Aspekty prawne



Informacje, w tym informacje zawarte w systemach komputerowych i telekomunikacyjnych podlegają ochronie w polskim prawie. Na początku należy podkreślić, że Konstytucja Rzeczypospolitej Polskiej w art. 49 zapewnia wolność i ochronę tajemnicy komunikowania się a ograniczenie tych wolności może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony.

Ochrona informacji została zapewniona także w kodeksie karnym. W rozdziale XXXIII zostały stypizowane przestępstwaprzeciwko ochronie informacji – art. od 265 kk do 269 c kk. Poniżej zostanie przytoczona treść tych przepisów a w dalszej części prezentacji zostaną bardziej szczegółowo omówione te, które dotyczą naruszenia prawa do informacji znajdujących się w systemach telekomunikacyjnych i informatycznych tj. art. 267 kk, 268 kk, 268a kk, 269 kk, 269a kk, 269 b kk i 269c kk.

Przestępczość komputerowa w polskim prawie

Art. 267. [Bezprawne uzyskanie informacji]

- § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
- § 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.
- § 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.
- § 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.
- § 5. Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego.

Przestępczość komputerowa w polskim prawie

Art. 268. [Utrudnianie zapoznania się z informacją]

- § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

- § 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.
- § 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową,

podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

- § 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

Przestępczość komputerowa w polskim prawie

Art. 268a. [Niszczenie danych informatycznych]

- § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych,

podlega karze pozbawienia wolności do lat 3.

- § 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową,

podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

- § 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Przestępczość komputerowa w polskim prawie

Art. 269. [Uszkodzenie danych informatycznych]

- § 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych,

podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

- § 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

Przestępczość komputerowa w polskim prawie

Art. 269a. [Zakłócenie systemu komputerowego]

Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Przestępczość komputerowa w polskim prawie

Art. 269b. [Wytwarzanie programów komputerowych]

- § 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 lub 2, art. 269a, art. 270 § 1 albo art. 270a § 1, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
- § 1a. Nie popełnia przestępstwa określonego w § 1, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia.
- § 2. W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy.

Przestępczość komputerowa w polskim prawie

Art. 269c. [Kontratyp działania w celu wykrycia błędów w zabezpieczeniach systemów informatycznych]

Nie podlega karze za przestępstwo określone w art. 267 § 2 lub art. 269a, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody.

Kiedy incydent jest przestępstwem?

- Bez uprawnienia
- Uzyskanie dostępu
- Przełamanie zabezpieczeń
- Zakładanie lub posługiwanie się urządzeniami specjalnymi
- Ujawnienie informacji

→

Procedury obsługi incydentów

1) Powiadamianie odpowiednich organów i zespołów
    - Wewnętrzne powiadomienia
    - Zewnętrzne powiadomienia
2) Priorytetyzacja incydentu
    - Ocena wpływu
    - Klasyfikacja incydentu
3) Zbieranie i postępowanie z dowodami
    - Zabezpieczenie miejsca incydentu
    - Dokumentacja dowodów
    - Bezpieczne przechowywanie dowodów
4) Działania naprawcze
    - Usunięcie zagrożenia
    - Wzmocnienie zabezpieczeń
    - Analiza incydentu
    - Komunikacja

Ochrona danych osobowych

Podstawy prawne

- Konstytucja RP:

1. Art. 47: Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.
2. Art. 51: Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. Władze publiczne nie mogą pozyskiwać, gromadzić ani udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.

→

Podstawy prawne

- Ustawa o ochronie danych osobowych:

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych reguluje kwestie związane z ochroną danych osobowych, ustanawiając między innymi Urząd Ochrony Danych Osobowych (UODO) jako organ nadzorczy.

→

Podstawy prawne

- RODO (GDPR):

Naruszenie ochrony danych osobowych, zgodnie z art. 4 pkt 12 RODO, oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Podstawy prawne

- RODO (GDPR):

Przykłady naruszeń:

- Utrata: Zgubienie nośnika danych (np. laptopa, pendrive'a) zawierającego dane osobowe.
- Nieautoryzowany dostęp: Dostęp do danych osobowych przez osobę nieuprawnioną.
- Ujawnienie: Przekazanie danych osobowych nieuprawnionym osobom lub podmiotom.
- Zniszczenie lub zmodyfikowanie: Przypadkowe lub celowe zniszczenie lub zmodyfikowanie danych osobowych.

Procedury zgłaszania naruszeń

1) Zgłoszenie naruszenia organowi nadzorczemu (UODO):

2) Zawiadomienie osób, których dane dotyczą

3) Dokumentacja naruszeń

Zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)

- CSIRT GOV
- CSIRT MON
- CSIRT NASK

→

Ransomware

Ransomware to rodzaj złośliwego oprogramowania (malware), które blokuje dostęp do systemu komputerowego lub danych poprzez szyfrowanie i żąda okupu za przywrócenie dostępu. Atak ransomware może prowadzić do poważnych konsekwencji dla organizacji, w tym utraty danych, przestojów operacyjnych oraz znacznych strat finansowych.

→

Ransomware

Charakterystyka ransomware:

1. Szyfrowanie danych
2. Żądanie okupu
3. Metody infekcji
4. Eskalacja uprawnień
5. Wyrafinowane techniki unikania wykrycia

→

Rekomendacje CERT Polska dotyczące postępowania po ataku

1) Izolacja zainfekowanych systemów
2) Nie płacenie okupu
3) Ocena zakresu szkód
4) Przywracanie danych z kopii zapasowych
5) Zgłoszenie incydentu
6) Usunięcie złośliwego oprogramowania
7) Zmiana haseł
8) Aktualizacja systemów i oprogramowania
9) Poprawa procedur bezpieczeństwa
10) Dokumentacja i analiza post-incident

Przykładowe procedury po incydencie

Kroki izolacji i dokumentacji incydentu

1. Izolacja incydentu
2. Dokumentacja incydentu

Strony i narzędzia pomocowe

1. Strony pomocowe
2. Narzędzia pomocowe

Procedury zgłaszania incydentu

1. Zgłoszenie do wewnętrznego zespołu
2. Zgłoszenie do organów zewnętrznych

Działania zapobiegawcze

1. Edukacja i szkolenia
2. Techniczne środki zabezpieczające
3. Polityki i procedury
4. Monitoring i audyt