# Co zrobić po incydencie?

**Akademia Górniczo-Hutnicza** im. Stanisława Staszica w Krakowie
AGH University of Krakow

04.06.2024

# Plan Prezentacji

- Definicja incydentu bezpieczeństwa
- Potrzeba reagowania na incydent
- Aspekty prawne
- Procedury obsługi incydentów
- Ochrona danych osobowych
- Zespoły reagowania na incydenty bezpieczeństwa komputerowego
- Ransomware
- Przykładowe procedury po incydencie

# Incydent bezpieczeństwa – definicja

Istnieje wiele źródeł i definicji, nieważne, po które sięgniemy, wspólny mianownik jest taki, że **incydent to każde zdarzenie, które przynosi lub może przynieść negatywny skutek (pośredni lub bezpośredni)**. Jaki to będzie skutek, zależy już od obszaru, w którym się poruszamy, oraz od rodzaju incydentu. Incydentem może być naruszenie bezpieczeństwa aktywów informacyjnych lub jakichkolwiek innych polityk bezpieczeństwa w organizacji. I tutaj wkracza procedura zarządzania incydentami bezpieczeństwa informacji, która pomaga wykrywać takie zdarzenia.

# Klasyfikacja incydentów bezpieczeństwa

- **krytyczny** – skutkuje znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych itd.
- **poważny** – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej
- **istotny** – ma istotny wpływ na świadczenie usługi cyfrowej
- **w podmiocie publicznym** – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny

# Przykładowe rodzaje incydentów bezpieczeństwa

- nieautoryzowany dostęp do sieci lub komputera
- wyciek informacji
- nadużycia na koncie na komputerze
- ataki malware lub DDOS
- kradzież lub zniszczenie urządzeń przetwarzających albo przechowujących informacje (w tym nośników danych)
- ujawnienie poufnych informacji na skutek np. zaniedbania lub braku rozwagi pracownika
- niedostępność lub niewłaściwe działanie systemów informatycznych

# Potrzeba reagowania na incydent

## Liczy się każda sekunda!

Cyberataki i inne incydenty bezpieczeństwa zagrażają wszystkim organizacjom. Nie znaczy to, że trzeba zaakceptować fakt iż jesteś nieunikalnie narażony. Powinno się stale oceniać, co może pójść nie tak i jak sobie z tym poradzić, ponieważ sposób, w jaki reagujesz na zdarzenie, może mieć wpływ na to, czy będziesz zmagać się z drobnymi zakłóceniami czy z poważnymi katastrofami.

# Zarządzanie incydentami - korzyści

- Szybsza reakcja na incydenty
- Zminimalizowanie negatywnego wpływu incydentów
- Szybkie przywrócenie zatrzymanych usług
- Zwiększenie bezpieczeństwa
- Redukcja kosztów

# Aspekty Prawne – Art.267

§ 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

# Procedury obsługi incydentów – priorytetyzacja incydentu

Nadanie priorytetu obsłudze incydentu jest prawdopodobnie najbardziej krytycznym punktem decyzyjnym w procesie obsługi incydentu. Ze względu na ograniczenia zasobów nie należy obsługiwać incydentów według kolejności zgłoszeń. Zamiast tego, postępowanie powinno być traktowane priorytetowo w oparciu o istotne czynniki, takie jak:

- Wpływ incydentu na funkcjonowanie organizacji
- Wpływ incydentu na informacje
- Możliwość odtworzenia po incydencie

# Procedury obsługi incydentów – powiadomienie odpowiednich organów i zespołów

Strony, które są zwykle powiadamiane, obejmują:

- CIO
- SAISO
- Lokalnego inspektora bezpieczeństwa informacji
- Inne zespoły reagowania na incydenty w organizacji
- Właściciela systemu
- Dział zasobów ludzkich
- Dział spraw publicznych
- Dział prawny
- Zespół reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)

# Procedury obsługi incydentów - zbieranie i postępowanie z dowodami

Zawsze należy prowadzić ewidencję dowodów. Za każdym razem, gdy dowody są przekazywane pomiędzy osobami, formularze kontroli dowodowej powinny określać szczegóły przekazania i zawierać podpis każdej ze stron. Należy prowadzić szczegółowy dziennik wszystkich dowodów, w tym:

- Informacje identyfikacyjne
- Nazwisko, stanowisko i numer kontaktowy każdej osoby, która zebrała lub zajmowała się materiałami dowodowymi
- Godzina i data każdego przypadku postępowania dowodowego
- Lokalizacje, w których przechowywano dowody

# Ochrona danych osobowych

- Jest to zbiór przepisów i regulacji prawnych, które mają na celu ochronę prywatności jednostek. Prawa dotyczą sposobów przetwarzania, tworzenia i zbierania danych osobowych
- Prawo do ochrony danych osobowych występuję też w konstytucji:

(art. 47.)

Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

(art. 51.)

1.Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.

2.Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.

# RODO = OROD = GDPR

RODO - Rozporządzenie o ochronie danych osobowych, stosuje się wymiennie z: OROD - Ogólne rozporządzenie o ochronie danych (po angielsku GDPR - General Data Protection Regulation).
Jego cel to pełna harmonizacja prawa w ramach UE i swobodny przepływ danych osobowych.
Rozporządzenie zostało przyjęte 27 kwietnia 2016 i weszło życie 25 maja 2018 we wszystkich krajach członkowskich UE.

# Główne zasady RODO

1. Zasada rzetelności, zgodności z prawem i przejrzystości.
2. Zasada ograniczenia celu przetwarzania.
3. Zasada minimalizacji danych.
4. Zasada prawidłowości.
5. Zasada ograniczenia przechowywania.
6. Zasada integralności i poufności.
7. Zasada rozliczalności.

# Wyrażanie zgody na przetwarzanie danych osobowych

Zgoda musi być:
- dobrowolna,
- konkretna,
- specyficzna (zgoda jest ważna, jeśli jest udzielona na konkretne użycie danych),
- świadoma (a zatem wymagana jest przejrzystość),
- wycofanie jej powinno być łatwe (użytkownik powinien mieć sposób sygnalizowania chęci wycofania zgody)

# Ustawa o ochronie danych osobowych

- Polska ustawa, uchwalona przez Sejm RP, regulująca kwestie prawne związane z ochroną danych osobowych, w szczególności zapewniająca stosowanie przepisów ogólnego rozporządzenia o ochronie danych (RODO).
- uchwalona 10 maja 2018 roku, weszła w życie 25 maja 2018 roku
- zastąpiła ustawę z 1997 roku
- urząd ochrony danych osobowych (UODO) - powstał wraz z nową ustawą

# Naruszenie ochrony danych osobowych

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

# CSIRT

CSIRT - computer security incident response team, po polsku: zespół reagowania na incydenty bezpieczeństwa komputerowego

W Polsce są 3 takie zespoły współpracujące ze sobą, lecz różniące się rolami i obsługiwanymi incydentami:

- CSIRT GOV
- CSIRT MON
- CSIRT NASK

# CSIRT GOV

Prowadzony przez agencję bezpieczeństwa wewnętrznego.
Obsługuje incydenty zgłaszane przez:
- jednostki sektora finansów publicznych
- Narodowy Bank Polski
- Bank Gospodarstwa Krajowego
- podmioty wchodzące w skład infrastruktury krytycznej

# CSIRT MON

Prowadzony przez ministerstwo obrony narodowej.
Obsługuje incydenty zgłaszane przez:
- Podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane
- Przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym
- Podmioty przekazane do właściwości CSIRT MON

# CSIRT NASK

Prowadzony przez Naukową i Akademicką Sieć Komputerową ( państwowy instytut badawczy ).
Poza obsługą incydentów, jego cel to działalność badawczo-rozwojowa.
Obsługuje incydenty zgłaszane przez:
- jednostki sektora finansów publicznych
- instytuty badawcze
- spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej
- dostawców usług cyfrowych, usług kluczowych
- osoby fizyczne

# Ransomware

Jest to oprogramowanie, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych (często poprzez techniki szyfrujące), a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego.

Pierwszym znanym programem typu ransomware był „AIDS” (znany również jako „PC Cyborg”), napisany w 1989 przez Josepha Poppa.

# Jak wygląda atak ransomware?

Ransomware przeważnie jest trojanem, wprowadzanym do systemu poprzez np. pobrany plik lub w wyniku luki w usłudze sieciowej.

Częste metody wyłudzenia pieniędzy:

- podszywanie się pod autorytety ( np. organy ścigania )
- fałszywe pokazywanie wygaśnięcie jakiejś licencji ( np. na system windows )
- próba przestraszenia użytkownika że jego komputer jest zainfekowany, i oferując naprawę za okup ( tzw. scareware )

# Co zrobić po ataku?

- izolacja maszyny - odłączyć od sieci, ale nie wyłączać ( pamięć RAM może być przydatna do analizy )
 - identyfikacja i eliminacja źródła infekcji
 - identyfikacja rodziny ransomware: pomóc mogą dwa narzędzia – nomoreransom.org oraz id-ransomware.malwarehunterteam.com
 - przywrócenie działania systemów
 - zgłoszenie incydentu: kontakt z CSIRT NASK, warto dołączyć zaszyfrowane pliki, notatkę z żądaniem okupu, próbkę ransomware, logi, oryginały zaszyfrowanych plików ( jeśli są ).

# Co zrobić po incydencie?

- dokonaj analizy, czy wyciek danych stanowi incydent czy też naruszenie ochrony danych osobowych
 - oceń ryzyko naruszenia praw i wolności osób dotkniętych zdarzeniem
- dokumentuj wszelkie naruszenia oraz podejrzenia naruszeń.
 - jeżeli ocena naruszenia wykaże konieczność zgłoszenia go do Prezesa Urzędu Ochrony Danych Osobowych (PUODO), jako administrator masz na to 72 godziny
- jeżeli naruszenie ochrony danych może mieć istostny wpływ na osoby, których dane uległy wyciekowi to masz obowiązek zawiadomienia tych osób o zdarzeniu

# Bibliografia


- https://www.gov.pl/
- https://www.isoqar.pl/pl/aktualnosci/bezpieczenstwo-informacji/zarzadzanie-reagowaniem-na-incydenty
- https://palestra.pl/pl/czasopismo/wydanie/2-2020/artykul/wspolczesne-systemy-informatyczne-a-typy-przestepstw-z-art.-267-kodeksu-karnego
- https://www.pbsg.pl/zarzadzanie-incydentami-bezpieczenstwa/
- https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf
- https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/krajowy-system-cyberbezpieczenstwa-18746756/roz-6
- https://www.rodosfera.pl
- https://lexdigital.pl/wyciek-danych-osobowych-jakie-dzialania-powinien-podjac-administrator