Z dziennika incydentów:
ochrona danych uczniów zaczyna się od świadomości zagrożeń

Andrzej Zieliński
Departament Kontroli i Naruszeń
Urząd Ochrony Danych Osobowych

Wstęp

Największym zagrożeniem dla bezpieczeństwa systemu informatycznego jest człowiek, który ma dobre intencje i zły dzień…

ciekawostka

74% naruszeń danych w 2023 roku miało źródło w błędzie człowieka

Verizon DBIR 2023.

Zanim zaczniemy: po co to wszystko?

Zrozumienie tego, co jest incydentem, to pierwszy krok do lepszej ochrony.

Nie ma tu winnych – są tylko ludzie, którzy po prostu nie mieli pełnej wiedzy.

ciekawostka

Aż 42% szkół nie ma spisanej procedury reagowania na incydenty.

NASK – „Cyberbezpieczeństwa w szkołach” 2023

Z życia wzięte — dane z incydentów

„Są tylko dwa rodzaje organizacji: te, które zostały zaatakowane, i te, które jeszcze nie wiedzą, że zostały”

John Chambers, były CEO Cisco Systems

ciekawostka

W 2024 roku Prezes UODO otrzymał 14 842 zgłoszenia naruszeń ochrony danych

Sprawozdanie z działalności UODO za 2024 rok

Skala zjawiska

W 2024 roku liczba zgłoszeń z sektora edukacji wzrosła o ponad 20%.—

Sprawozdanie z działalności UODO za 2024 rok

ciekawostka

Liczba ataków hakerskich na polskie placówki oświatowe wzrosła ponad pięciokrotnie — i to tylko w ciągu 8 miesięcy 2025 roku w porównaniu do całego roku 2023.

Serwisu Samorządowego PAP

Ranking incydentów

- *Omyłkowe przesłanie informacji*
- *Włamania na konta*
- *Nieodebranie uprawnień*
- *Omyłkowa publikacja danych w Internecie*
- *Błędy w konfiguracji systemów*
- *Atak ransomware*
- *Utrata nośników*
- *Phishing*

Omyłkowe przesłanie informacji

„Arkusz ocen wysłany do innego rodzica”

„Dane rekrutacyjne do błędnej placówki”

ciekawostka

Przesłanie danych osobowych do niewłaściwego odbiorcy” stanowiło aż 1/3 wszystkich naruszeń zgłoszonych do UODO w 2023 roku.

Włamanie na konto

„W godzinach wieczornych zalogowano się na konto pracownika szkoły, z którego zaczęto wysyłać spam”

„Podczas ferii zimowych zostały dopisane oceny uczniom w wybranych klasach”

ciekawostka

*Według raportu NordPass 2024, najpopularniejszym hasłem na świecie (i w Polsce) pozostaje niezmiennie:„**123456**”*

Nieodebranie uprawnień

„Po rozwiązaniu stosunku pracy, byli pracownicy logowali się do Rejestru Sprawców Przestępstw na Tle Seksualnym”

„Podmiot przetwarzający nie poinformował szkoły, że dwóm byłym pracownikom trzeba odebrać dane do logowania”

ciekawostka

1 na 5 szkół w Polsce nie usuwała kont byłych pracowników po zakończeniu pracy.

Źródło: NASK, „Cyberbezpieczeństwa w szkołach 2024

Omyłkowa publikacja danych w Internecie

„Opublikowano w BIP zarządzenia z danymi nauczycieli i ucznia bez ich anonimizacji”

„Omyłkowo opublikowano na stronie szkoły zaświadczenie zawierające : imię, nazwisko, PESEL, adres zamieszkania”

ciekawostka

W 2023 r. UODO odnotował kilkadziesiąt przypadków, w których dane uczniów były dostępne publicznie — np. na stronie internetowej szkoły.

Sprawozdanie z działalności UODO za 2023 rok

Błędy w konfiguracji systemów

„W wyniku błędu konfiguracji w systemie poczty część uczniów mogła zobaczyć pole „Centrum kosztów” zawierające numer PESEL.

„W wyniku zmiany konfiguracji Włączono indeksowanie katalogów, przez co ich zawartość była publicznie widoczna.

ciekawostka

Według danych z USA - 25% naruszeń danych w 2025 r. wynikało z błędów konfiguracji i innych pomyłek

Verizon Data Breach Investigations Report 2025

Atak ransomware

„Atak ransomware na serwery ESX przez zaszyfrowanie maszyn wirtualnych”

„Po udostępnieniu zdalnego dostępu przez RDP do komputera z danymi kadrowymi, doszło do ataku ransomware”

ciekawostka

W 2025 roku ransomware atakowało średnio co 1,3 godziny

Comparitech – Ransomware Roundup Q3 2025

Atak ransomware

- *65% ataków ransomware rozpoczęło się od wykorzystania luk w systemach IT — głównie niezałatanych błędów w oprogramowaniu (CVE, zero-day).*
- *Tylko 54% organizacji odzyskało dane z kopii zapasowej po ataku — reszta albo zapłaciła okup, albo straciła dane bezpowrotnie.*

Źródło: The State of Ransomware 2025, Sophos

Atak ransomware

Profilaktyka:

1. ***Aktualizuj systemy i programy***
2. ***Twórz kopie zapasowe danych***
3. ***Uważaj na załączniki i linki***
4. ***Ogranicz dostęp do systemów: „Zasada najmniejszych uprawnień”***
5. ***Testuj zdalne dostępy***

Utrata nośników

„Kradzież laptopa”

„Znaleziono pendrive z danymi osobowymi”

ciekawostka

Według ENISA aż 12% naruszeń danych w szkołach wynika z utraty nośnika..

ENISA Threat Landscape 2023

Phishing

„Pracownik kliknął w fałszywy link”

„E-mail z informacją o „aktualizacji hasła” przekierował na fałszywą stronę logowania”

ciekawostka

AI zwiększyło liczbę phishingów o 1 265%

Forbes – AI Is Amping Up Phishing 2022

Phishing to nie technologia — to psychologia

X w. p.n.e. – Koń trojański

XIII w. – Fałszywe listy królewskie

Phishing to nie technologia — to psychologia

- ***Strach***
- ***Pośpiech / presja czasu***
- ***Ciekawość***
- ***Ufność***
- ***Autorytet***
- ***Litość / empatia***
- ***Chciwość / okazja***

Brak świadomości incydentu

Najgroźniejsze incydenty to te, których nikt nie zauważył.

ciekawostka

30% incydentów zgłaszanych jest po terminie

Sprawozdanie z działalności UODO za 2024 rok

Jak rozpoznać incydent?

Nie każdy błąd to incydent, ale każdy incydent wymaga reakcji

- **Incydent to naruszenie poufności, integralności lub dostępności danych.**
- **Wątpliwości? – lepiej zgłosić niż zignorować**

ciekawostka

Pracownicy nie zgłaszają średnio 41 % incydentów

Keeper Security, 2023, badanie opisane w ITBrew

Co robić po incydencie?

3 kroki po wykryciu incydentu

1. **Zabezpiecz dane – odłącz urządzenie, zmień hasło, usuń dostęp**
2. **Zgłoś incydent – do IOD, dyrektora lub administratora systemu**
3. **Wyciągnij wnioski – przeanalizuj przyczynę i wprowadź poprawki**

ciekawostka

Tylko 55% organizacji posiada w pełni udokumentowany plan reakcji na

JumpCloud, Incident Response Statistics to Know in 2025

Najczęstsze błędy po incydencie

- **Zbyt długo czekamy z reakcją („może się samo naprawi”)**
- **Ukrywamy zdarzenie z obawy przed krytyką**
- **Nie informujemy właściwych osób (IOD, administratora)**
- **Nie dokumentujemy zdarzenia**
- **Wracamy do pracy bez analizy przyczyn**

ciekawostka

W jednej z brytyjskich szkół (2022) pracownik po przypadkowym wysłaniu e-maila z danymi uczniów do niewłaściwego adresata nie poinformował IOD, tylko wysłał kolejnego maila z prośbą o „usunięcie wiadomości”.

Jak zwiększyć bezpieczeństwo w szkole?

5 prostych zasad, które naprawdę działają

1. *Procedury*
2. *Szkolenia*
3. *Silne hasła*
4. *Zasada najmniejszych uprawnień*
5. *Kopie zapasowe*

Przykłady z innych krajów

- *Wielka Brytania (2023): Inns of Court College of Advocacy – błędne udostępnienie danych studentów*
- *Australia (2021): Uniwersytet Adelaide – wysłanie danych osobowych do niewłaściwego adresata*
- *Wielka Brytania (2023): Szkoła wysłała dane uczniów do niewłaściwego odbiorcy przez e-mail*

Podsumowanie

1. *Wiedza to pierwszy krok*
2. *Działanie — drugi*
3. *Odwaga, by je połączyć — trzeci*

Dziękuję za uwagę

Urząd Ochrony Danych Osobowych
ul. Moniuszki 1A, 00-014 Warszawa
www.uodo.gov.pl/tdts

URZĄD OCHRONY DANYCH OSOBOWYCH