2023-02-17

# Zawiadomienie publiczne o naruszeniu ochrony danych osobowych

**Zawiadomienie publiczne o naruszeniu ochrony danych osobowych**

Miejski Ośrodek Pomocy Społecznej w Zgierzu jako administrator danych osobowych informuje, że 13 lutego 2023 r. miał miejsce atak na infrastrukturę sieciową Miejskiego Ośrodka Pomocy Społecznej im. bł. o. Rafała Chylińskiego w Zgierzu (95-100 Zgierz, ul. Długa 56) przy użyciu oprogramowania szyfrującego.

W wyniku tego zdarzenia utraciliśmy dostępność do systemów informatycznych oraz danych. Dane osobowe znajdujące się w naszym administrowaniu uległy zaszyfrowaniu w  znaczącej części i trwają prace nad ich przywróceniem.

Wszystkie dane osobowe znajdujące się w dokumentacji papierowej są dostępne. Naruszenie dotyczy danych w systemach teleinformatycznych.

Z przeprowadzonej dotychczas analizy wynika, że doszło do utraty dostępności (nie mamy możliwości wglądu w dane osobowe). Brak jest wskazań, aby doszło do wycieku danych (przejęcia ich przez osoby nieuprawnione) oraz brak jest informacji, aby dane takie zostały wykorzystane w nieuprawiony sposób.

Z uwagi na zakres i skalę tego co się stało, o zdarzeniu poinformowaliśmy Prezesa Urzędu Ochrony Danych Osobowych (PUODO), Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT NASK), a także Prokuraturę.

Informacji na temat zdarzenia oraz odpowiedzi na pytania udzielamy drogą mailową i telefoniczną poprzez wyznaczone osoby:

**Panią Renatę Wolską – Dyrektora Ośrodka: tel. 693-001-895 mail: renata.wolska@mopszgierz.pl**

**Panią Aleksandrę Karpińską – Inspektora Ochrony Danych: tel. 693-002-231 mail : iodo@mopszgierz.pl**

Ponadto w ramach osobnego komunikatu będziemy publikować aktualizacje informacji oraz odpowiedzi na pojawiające się pytania.

Dokładamy wszelkich starań, aby przywrócić funkcjonowanie systemów. W prace zaangażowano zespół Ośrodka oraz specjalistyczne podmioty zewnętrzne.

**Jakie działania zostały podjęte po wykryciu naruszenia?**

- Dokonano zgłoszenia do CSRIT NASK, Prezesa UODO, Prokuratury,
- Podjęto działania weryfikujące i działania mające na celu przywrócenie sprawności funkcjonowania systemów,
- Dokonano identyfikacji rodzaju złośliwego oprogramowania,
- Trwają prace nad analizą dzienników sieciowych,
- Trwa sprawdzanie infrastruktury komputerowej,
- Podjęto działania naprawcze w zakresie kopii zapasowych i odzyskania danych – także przy współpracy z wyspecjalizowanym podmiotem zewnętrznym,
- Nawiązano kontakt z napastnikami i prowadzona jest z nimi korespondencja,
- Wyznaczono osoby do kontaktu i udzielania informacji,
- Dokonano wstępnej oceny ryzyka i powiadomienia publicznego o wystąpieniu naruszenia.

**Jakie są konsekwencje tego naruszenia?**

Ośrodek utracił dostęp do części systemów informatycznych oraz baz danych zawierających dane osobowe. Może to skutkować przerwą w możliwości działania i świadczenia usług dla mieszkańców.

**Jaki wpływ na osoby korzystające z MOPS ma wpływ to zdarzenie?**

Wystąpią trudności lub brak możliwości realizowania części usług – pomoc społeczna, fundusz alimentacyjny, dodatki mieszkaniowe oraz kadry.

Ponieważ brak jest potwierdzenia o wycieku danych lub wykorzystaniu ich przez osoby nieuprawione – cały czas trwają prace mające ostatecznie potwierdzić, że taka sytuacja nie ma miejsca. Zalecamy jednak zachowanie szczególnej ostrożności.

**Czy moje dane są bezpieczne? Czy moje dane wyciekły?**

Dotychczasowa analiza nie wskazuje, że doszło do utraty dostępności danych, czyli Ośrodek nie

ma dostępu do systemów oraz danych w nich zebranych. Brak jest potwierdzenia, aby dane osobowe zostały wykradzione lub ktoś posługiwał się nimi w nieuprawiony sposób. Ze względu na powagę sytuacji sprawdzenia są kontynuowane, a sytuacja jest monitorowana.

**Czy można normalnie korzystać z pomocy MOPS?**

Ośrodek nadal świadczy wsparcie na rzecz mieszkańców, jednak wystąpiły duże ograniczenia w działaniu systemów informatycznych oraz brak dostępu do danych w formie elektronicznej. Pracujemy nad szybkim przywróceniem dostępności.

**Czy zgłoszono sprawę do organów ścigania?**

Sprawa została zgłoszona do Prokuratury. Ponadto do Prezesa UODO oraz Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT NASK).

Podjęto też współpracę z zewnętrznym podmiotem specjalistycznym.

**Co to za atakujący? Kto dokonał ataku i skąd wiadomo, że to atak?**

Na dzień dzisiejszy nie jesteśmy w stanie ustalić kim są osoby, które dokonały ataku. Trwa ustalanie faktycznego źródła zdarzenia.

Doszło do zaszyfrowania zasobów, a następnie zażądano okupu za ich odszyfrowanie. Prowadzone są rozmowy i podejmowane próby uzyskania informacji. Ustalono ponad wszelką wątpliwość, że atakującym chodzi o uzyskanie pieniędzy.