

Ważny komunikat: **Prewencyjne ostrzeżenie dla Pacjentów i Podmiotów współpracujących dotyczące bezpieczeństwa danych**

Szanowni Pacjenci,

zostaliśmy poinformowani przez firmę Fakturownia sp. z o.o. - zewnętrznego dostawcę oprogramowania wspierającego prowadzenie rozliczeń, z którego korzysta m. in. nasza placówka, o wykryciu incydentu bezpieczeństwa (cyberataku) w jego systemach informatycznych.

Dostawca oprogramowania prowadzi obecnie intensywne dochodzenie techniczne mające na celu ustalenie skali incydentu, tj. czy do danych naszych pacjentów lub podmiotów współpracujących dostęp miały osoby nieuprawnione, a jeśli tak – jakiej grupy osób i jakiego zakresu informacji to dotyczy.

Kierując się zasadą pełnej transparentności oraz troską o Państwa bezpieczeństwo, nie czekamy na ostateczne wyniki dochodzenia prowadzonego przez ekspertów i służby. Chcemy dać Państwu możliwość podjęcia natychmiastowych działań prewencyjnych i ochronnych.

Aby całkowicie wyeliminować ryzyko ewentualnego wykorzystania Państwa danych, rekomendujemy wykonanie następujących kroków:

1. prewencyjne zastrzeżenie numeru PESEL – to bezpłatna i najskuteczniejsza metoda blokady wprowadzanej natychmiast i bezpłatnie w aplikacji mObywatel, przez rządowy portal obywatel.gov.pl lub osobiście w lokalnym urzędzie; warto podkreślić, że zastrzeżenie numeru PESEL nie blokuje możliwości korzystania ze świadczeń medycznych, w tym realizacji recept w aptekach czy wizyt lekarskich,
2. aktywacja alertów w Biurze Informacji Kredytowej (BIK) – usługa ta powiadomi Państwa SMS-em o każdej próbie sprawdzenia historii kredytowej,
3. zwiększona czujność przy odbieraniu podejrzanych wiadomości SMS, wiadomości e-mail oraz telefonów od nieznanych osób, w tym unikanie otwierania linków i załączników w nieoczekiwanych wiadomościach, podawania haseł, kodów weryfikacyjnych, kodów BLIK czy danych kart,
4. przy pojawieniu się telefonów „z banku”, „z urzędu” lub „z Fakturowni” rozłączanie się i oddzwanianie na numer z oficjalnej strony,
5. potwierdzanie innym, znanym wcześniej, kanałem komunikacji wszelkich prośb o pilny lub nietypowy przelew, czy zmianę rachunku bankowego,
6. przesyłanie podejrzanych SMS-ów do CERT Polska na numer 8080,
7. sprawdzanie rachunków kontrahentów na białej liście podatników VAT.

Co robimy w tej sprawie?

Jesteśmy w kontakcie z dostawcą oprogramowania i żądamy od niego natychmiastowych, szczegółowych wyjaśnień oraz raportów z prowadzonego przez niego dochodzenia.

Gdy tylko otrzymamy oficjalny raport techniczny określający dokładną skalę zdarzenia oraz potwierdzający zakres danych, zaktualizujemy ten komunikat, a osoby bezpośrednio dotknięte incydem powiadomimy zgodnie z przepisami prawa.

W razie pytań pozostajemy do Państwa dyspozycji pod adresem golddentica@gmail.com.

Bieżące informacje na temat incydentu można również uzyskać na stronie przygotowanej przez firmę FELG Software sp. z o.o. pod adresem <https://status.felg.cloud/incydent>.

*dr n. med. Agnieszka Kozak-Rusinek
Kierownik Kliniki*