LEKARZ DOMOWY
SZUBIN, UL. WINNICA 3A

INFORMACJA DLA PACJENTÓW

dotycząca incydentu bezpieczeństwa w systemach MyDr

Szanowni Państwo,

informujemy, że firma MyDr sp. z o.o. z siedzibą w Warszawie, będąca dostawcą systemów informatycznych wykorzystywanych przez naszą placówkę medyczną, poinformowała o wystąpieniu incydentu cyberbezpieczeństwa będącego wynikiem celowego, zewnętrznego działania o charakterze przestępczym.

Oprogramowanie będące przedmiotem cyberataku wykorzystujemy jedynie do niewielkiej części naszej działalności leczniczej, jaką są prywatne gabinety specjalistyczne. W pozostałym zakresie, tj. w prowadzeniu podstawowej opieki zdrowotnej, korzystamy z oprogramowania informatycznego innego dostawcy.

Z informacji przekazanych przez MyDr wynika, że incydentem została objęta część danych przetwarzanych w systemach tego dostawcy. MyDr prowadzi obecnie szczegółową analizę zdarzenia, której celem jest ustalenie m.in. zakresu danych objętych incydentem oraz klientów, których zdarzenie dotyczy.

Na chwilę obecną nie otrzymaliśmy potwierdzenia, że incydent objął dane osobowe pacjentów naszej placówki. Nie ma również obecnie podstaw do stwierdzenia, że dane konkretnego pacjenta zostały ujawnione lub wykorzystane przez osoby nieuprawnione.

Ze względu na charakter zdarzenia oraz możliwość, że mogło ono dotyczyć danych przetwarzanych przez MyDr na rzecz naszej placówki, zdecydowaliśmy się poinformować Państwa o zaistniałej sytuacji.

Co robimy?

Monitorujemy rozwój sytuacji oraz oczekujemy od MyDr na przekazanie informacji pozwalających jednoznacznie ustalić, czy incydent objął dane przetwarzane w związku z działalnością naszej placówki, a jeżeli tak – jakich osób i jakiego zakresu danych dotyczył.

Po uzyskaniu takich informacji dokonamy odpowiedniej oceny zdarzenia i podejmiemy działania wymagane przepisami dotyczącymi ochrony danych osobowych. O istotnych ustaleniach oraz dalszym rozwoju sytuacji będziemy Państwa informować. Jeżeli zostanie potwierdzone, że incydent dotyczył danych naszych pacjentów i będzie wymagał podjęcia przez Państwa określonych działań, przekażemy odpowiednie informacje oraz zalecenia.

Zwróciliśmy się do dostawcy oprogramowania z wnioskiem o wskazanie, czy dane naszych Pacjentów objęte były cyberatakiem – na ten moment oczekujemy na oficjalną odpowiedź.

Zaangażowaliśmy w sprawę zespół naszych informatyków oraz zewnętrzną firmę, która świadczy dla nas wymagane ustawą o ochronie danych osobowych obowiązki inspektora ochrony danych osobowych. Postępujemy zgodnie z ich zaleceniami.

Co warto zrobić?

Na obecnym etapie nie ma potrzeby podejmowania pochopnych działań. Niezależnie jednak od opisanego incydentu zachęcamy do stosowania podstawowych zasad bezpieczeństwa, które ograniczają ryzyko nieuprawnionego wykorzystania danych osobowych:

• warto mieć zastrzeżony numer PESEL – jest to dobre rozwiązanie prewencyjne niezależnie od obecnego incydentu. Zastrzeżenia można dokonać m.in. za pośrednictwem aplikacji lub serwisu mObywatel, a w razie potrzeby można je czasowo cofnąć;

• należy stosować unikalne i silne hasła – nie należy używać tego samego hasła w kilku różnych serwisach;

• należy korzystać z uwierzytelniania wieloskładnikowego (MFA/2FA) wszędzie tam, gdzie jest ono dostępne;

• nie należy przekazywać haseł, kodów SMS, kodów BLIK ani innych danych służących do uwierzytelnienia, nawet jeżeli osoba kontaktująca się twierdzi, że reprezentuje bank, placówkę medyczną, urząd lub inną znaną instytucję;

• należy zachować szczególną ostrożność wobec wiadomości SMS, e-maili i połączeń telefonicznych, zwłaszcza dotyczących wizyt, recept, skierowań, wyników badań, płatności lub konieczności „pilnego potwierdzenia" albo „aktualizacji" danych;

• nie należy klikać w podejrzane linki i nie należy otwierać nieoczekiwanych załączników – w razie wątpliwości należy skorzystać z oficjalnej strony, aplikacji lub oficjalnego numeru telefonu danej instytucji;

• należy pamiętać, że sam fakt, iż osoba kontaktująca się zna część danych którymi się posługuje, nie potwierdza jej wiarygodności; • należy zwracać uwagę na nietypową aktywność na kontach internetowych, poczcie elektronicznej oraz rachunkach bankowych i niezwłocznie reagować na nieznane logowania, operacje lub próby zmiany haseł.

W przypadku otrzymania podejrzanej wiadomości lub telefonu, w którym ktoś powołuje się na naszą placówkę, rekomendujemy przerwanie kontaktu i samodzielne skontaktowanie się z placówką za pośrednictwem oficjalnych danych kontaktowych.

Powyższe zalecenia mają charakter prewencyjny i nie oznaczają, że wskazane rodzaje danych – w szczególności numer PESEL, hasła lub dane dostępowe – zostały objęte incydentem.

Na bieżąco monitorujemy sytuację i będziemy informować Państwa o nowych, istotnych ustaleniach dotyczących incydentu.

Z poważaniem

Zespół Przychodni Lekarz Domowy