INFORMACJA

dot. incydentu ujawnienia danych osobowych 20 tys. funkcjonariuszy zbieranych w ramach akcji szczepień przeciw COVID-19

W związku z doniesieniami medialnymi oraz komunikatem wydanym przez Rządowe Centrum Bezpieczeństwa po potencjalnym incydencie naruszenia ochrony danych osobowych związanym z ujawnieniem w sieci danych ponad 20 tys. funkcjonariuszy i pracowników rządowych zbieranych w ramach akcji szczepień przeciw COVID-19, informujemy:

1. Z uwagi, że incydent ten najprawdopodobniej dotyczy również danych osobowych strażaków, Zespół Eksportów Komendanta Głównego PSP ds. ochrony danych osobowych prowadzi bieżący monitoring zaistniałej sytuacji;
2. Całość postępowania z incydentem prowadzona jest przez Rządowe Centrum Bezpieczeństwa. O decyzjach i informacjach uzyskanych z RCB będziemy informować na bieżąco;
3. Na chwilę obecną nie posiadamy informacji, których osób dotyczy incydent, ale wszystko na to wskazuje, że naruszenie może dotyczyć wyłącznie osób, które zadeklarowały chęć zaszczepienia w okresie od 12 do 20 kwietnia 2021 roku (około 4000 wpisów). Zakres danych, które mogły zostać udostępnione to:
   - Imię i nazwisko,
   - Numer telefonu,
   - Pełna nazwa jednostki,
   - PESEL,
   - Adres (Ulica i numer budynku, Kod pocztowy, Miejscowość) dot. osoby wprowadzającej dane do bazy,
   - Adres e-mail pracownika wprowadzającego dane do bazy,
   - Imię i nazwisko pracownika wprowadzającego dane do bazy,
   - Numer telefonu komórkowego do pracownika wprowadzającego dane do bazy;
4. Należy mieć na względzie, że zakres ujawnionych danych może prowadzić do potencjalnych wyłudzeń, ataków socjotechnicznych oraz związanych z tym szkód majątkowych i niemajątkowych;
5. Prosimy zwiększyć czujność w zakresie analizy treści otrzymywanych w smsach i emailach, szczególnie tych, które zawierają linki (odesłania) do innych stron. Strony te mogą zawierać formularze wyłudzające dane osobowe lub zawierać złośliwe oprogramowanie pozwalające przejąć kontrolę nad urządzeniem. Zagrożenie to może dotyczyć również portali społecznościowych i wykorzystania tzw. ataków socjotechnicznych polegających na próbie podszycia się pod inne osoby. Zwracamy również uwagę, że mogą pojawić się smsy lub e-maile informujące np. o zmianie terminu szczepienia i konieczności wejścia na fałszywy link.
6. Ponadto informujemy, że w Polsce funkcjonuje kilka różnych usług, dzięki którym można utrudnić oszustom wzięcie np. pożyczki na nielegalnie pozyskane dane osobowe np. numer PESEL. Niestety na dzień dzisiejszy usługi te, nie tworzą jednolitego systemu. Dlatego proponujemy zapoznać się ze szczegółami poszczególnych usług i rozważenie ich stosowania, jako dodatkowego zabezpieczenia swoich danych osobowych. Przykładami usług chroniących dane osobowe są m. in. Alerty BIK, ChrońPESEL, czy BezpiecznyPesel. W zdecydowanej większości usługi te są dodatkowo płatne.

Mając na względzie powagę zaistniałej sytuacji prosimy, aby powyższą informację przekazać osobom, których dane mogły zostać upublicznione.

Zespół Ekspertów
Komendanta Głównego PSP
ds. ochrony danych osobowych