KOMUNIKAT • DATA PUBLIKACJI: 3 listopad 2026

Cyberatak na systemy Farmutil

Ważne informacje dla obecnych i byłych pracowników oraz osób wskazanych w dokumentacji kadrowej

W skrócie

CO SIĘ STAŁO?

Atak ransomware

29 października 2026 r. wykryliśmy atak na naszą infrastrukturę informatyczną. Część danych została zaszyfrowana.

CZEGO JESZCZE NIE WIEMY?

Czy dane wyciekły

Sprawdzamy, czy sprawcy odczytali lub skopiowali dane. Na tym etapie nie możemy tego wykluczyć.

CO ZROBIĆ TERAZ?

Trzy kroki

1. Zastrzeżenie numeru PESEL.

2. Nieprzekazywanie nikomu haseł ani kodów.

3. Weryfikacja nieoczekiwanych kontaktów.

Szanowni Państwo,

Zakład Rolniczo-Przemysłowy „FARMUTIL HS” S.A. padł ofiarą przestępczego ataku ransomware na infrastrukturę informatyczną. Atak wykryliśmy 29 października 2026 r. Według wstępnych ustaleń mógł rozpocząć się dzień wcześniej. Dokładny przebieg zdarzenia jest ustalany.

Sprawcy zaszyfrowali dane i zablokowali dostęp do części zasobów. Sprawdzamy, czy osoby nieuprawnione mogły także odczytać, skopiować lub ujawnić dane. **Na obecnym etapie nie możemy tego wykluczyć.**

Rozumiemy Państwa niepokój i przepraszamy za zaistniałą sytuację. Choć to Spółka stała się celem przestępczego ataku, czujemy się w pełni odpowiedzialni za zaistniałą sytuację, ochronę powierzonych nam danych oraz zapewnienie Państwu informacji i wsparcia. Przekazujemy komunikat przed zakończeniem analizy, aby mogli Państwo od razu podjąć działania ochronne. Prosimy przede wszystkim o zastrzeżenie numeru PESEL oraz ostrożność wobec nieoczekiwanych telefonów, SMS-ów i wiadomości e-mail.

01 Kogo dotyczy zdarzenie

Weryfikacja obejmuje dokumentację kadrową i płacową dotyczącą:

- obecnych pracowników Spółki,
- byłych pracowników Spółki,
- osób, których dane pracownicy przekazali Spółce, np. członków rodziny, osób zgłoszonych do ubezpieczenia, osób uprawnionych do świadczeń lub wskazanych do kontaktu w nagłych sytuacjach.

Jakie dane mogły zostać objęte atakiem

Zależnie od zawartości poszczególnych dokumentów potencjalnie zagrożone mogą być:

Kategoria	Przykłady danych
Dane identyfikacyjne	imię i nazwisko, PESEL, data urodzenia, imiona rodziców, nazwisko rodowe matki, obywatelstwo, seria i numer dokumentu tożsamości
Dane kontaktowe	adres zamieszkania lub pobytu, numer telefonu, adres e-mail
Zatrudnienie i finanse	informacje o zatrudnieniu i wynagrodzeniu, numer rachunku bankowego, informacje o sytuacji majątkowej
Dane o zdrowiu	w zakresie zawartym w dokumentacji pracowniczej
Dane dostępowe	nazwy użytkowników i hasła do systemów - o ile znajdowały się w zasobach objętych atakiem
Dane osób bliskich	w zakresie zawartym w dokumentacji kadrowej

ZAKRES JEST WSTĘPNY

Nie oznacza to, że wszystkie wymienione dane każdej osoby zostały objęte atakiem lub ujawnione. Ustalamy dokładny zakres zdarzenia, liczbę osób i dokumentów oraz okres, którego dotyczą dane.

02 Jakie zagrożenia warto znać

WYCIEK NIE ZOSTAŁ POTWIERDZONY

Poniższe ryzyka dotyczą sytuacji, w której sprawcy odczytali lub skopiowali dane. Zakres incydentu jest nadal weryfikowany.

Jeżeli doszło do nieuprawnionego pozyskania danych, mogą one zostać wykorzystane do:

Kradzieży tożsamości

Próby uzyskania pożyczki, kredytu, zakupu na raty lub zawarcia innej umowy na cudze dane.

Podszywania się

Kontakty z instytucjami, usługodawcami lub innymi osobami w Państwa imieniu.

Wiarygodnych oszustw

Wiadomości od rzekomego pracodawcy, działu kadr, banku, ZUS, Policji.

Wyłudzeń pieniędzy i kodów

Także z wykorzystaniem informacji o wynagrodzeniu lub rodzinie.

Przejęcia kont

Jeżeli te same dane logowania były używane również w innych serwisach.

Naruszenia prywatności

Ujawnienie informacji o zdrowiu lub finansach - stres, szkoda reputacyjna, dyskryminacja, szantaż.

Zagrożenia mogą dotyczyć również osób wskazanych w dokumentacji przez pracowników. Utrata dostępu do części zasobów może ponadto powodować opóźnienia w obsłudze spraw kadrowych, wydawaniu dokumentów lub realizacji innych spraw wymagających dostępu do zaatakowanych systemów.

Opisujemy możliwe następstwa, a nie potwierdzone przypadki wykorzystania Państwa danych. Numer PESEL w połączeniu z innymi danymi może ułatwiać próby podszywania się i wyłudzeń. Dlatego zalecamy działania ochronne już teraz.

ZNAJOMOŚĆ PAŃSTWA DANYCH NIE POTWIERDZA TOŻSAMOŚCI ROZMÓWCY

Oszuści mogą znać PESEL, adres, wynagrodzenie lub dane bliskich. W razie wątpliwości należy zakończyć rozmowę i samodzielnie oddzwonić na znany wcześniej numer instytucji.

03 Sześć działań ochronnych

Rekomendujemy podjęcie poniższych działań już teraz, bez oczekiwania na zakończenie analizy.

1

Zastrzeżenie numeru PESEL

Instrukcja wideo w YouTube: https://www.youtube.com/watch?v=Mg3lPNeGtus

Bezpłatnie i od razu - w aplikacji mObywatel, przez internet (gov.pl) lub w dowolnym urzędzie gminy. Szczegółowa instrukcja: https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie

Zastrzeżenie ogranicza ryzyko określonych nadużyć finansowych, ale nie usuwa ujawnionych danych i nie chroni przed wszystkimi rodzajami oszustw.

2

Ostrożność wobec telefonów i wiadomości

Prosimy nie przekazywać nikomu haseł, kodów SMS i BLIK ani danych do bankowości, nie instalować programów do zdalnego dostępu i nie wykonywać przelewów na „bezpieczne konto".

W związku z incydentem Farmutil nie będzie prosić telefonicznie, SMS-em ani e-mailem o hasła, kody, dane do bankowości ani o wykonanie przelewu. Kontakt powołujący się na Spółkę należy sprawdzić w punkcie pomocy wskazanym w tym komunikacie.

3

Kontrola rachunków i powiadomień

Warto zwracać uwagę na nieznane transakcje, wnioski kredytowe, umowy, wezwania do zapłaty i korespondencję o niezamówionych usługach. W razie podejrzenia nadużycia należy skontaktować się bezpośrednio z bankiem lub usługodawcą.

Można rozważyć alerty o próbach uzyskania finansowania, np. oferowane przez BIK - takie usługi mogą być odpłatne i nie zastępują zastrzeżenia PESEL.

4

Zmiana haseł

Jeżeli hasło używane w pracy było używane również prywatnie, prosimy zmienić je w pozostałych usługach a przede wszystkim w poczcie elektronicznej. Zalecamy stosowanie różnych haseł i włączenie uwierzytelniania wieloskładnikowego. Zmiany kont służbowych należy wykonywać zgodnie z instrukcjami działu IT.

5

Poinformowanie bliskich

Prosimy przekazać tę informację osobom, których dane zostały przez Państwa podane Spółce. Pełnoletnie osoby z numerem PESEL mogą samodzielnie go zastrzec. Standardowa usługa zastrzegania PESEL jest przeznaczona dla osób pełnoletnich, w przypadku dzieci należy szczególnie uważać na próby wyłudzania danych i pieniędzy.

6

Reakcja na podejrzenie oszustwa

Jeżeli doszło do przekazania danych do bankowości lub kodu autoryzacyjnego albo wykonania podejrzanego przelewu należy niezwłocznie skontaktować się z bankiem. Podejrzenie przestępstwa prosimy zgłosić Policji, zachować wiadomości, numery telefonów i potwierdzenia oraz poinformować punkt pomocy Spółki.

04 Co robi Farmutil

Niezwłocznie po wykryciu ataku podjęliśmy działania w celu ograniczenia jego skutków i zabezpieczenia systemów. Prowadzimy analizę zdarzenia, działania naprawcze oraz odtwarzanie danych z kopii zapasowych. Weryfikujemy zakres naruszenia i jego skutki dla osób, których dane przetwarzamy.

Zdarzenie zgłosiliśmy Prezesowi Urzędu Ochrony Danych Osobowych, właściwemu zespołowi CSIRT w tym Policji. Pozostajemy z nimi w stałym kontakcie i podejmujemy współpracę w zakresie obsługi incydentu. Przekazujemy dostępne informacje oraz kolejne ustalenia potrzebne do wyjaśnienia zdarzenia i ograniczenia jego skutków.

URZĄD OCHRONY DANYCH OSOBOWYCH	30 LAT CERT.PL NASK	POLICJA
PREZES UODO	**CSIRT**	**POLICJA**
Ochrona danych osobowych Zgłoszenie naruszenia Stały kontakt i współpraca	Reagowanie na cyberincydent Zgłoszenie zdarzenia Stały kontakt i współpraca	Wyjaśnienie przestępstwa Zgłoszenie zdarzenia Stały kontakt i współpraca

Stale rozwijamy zabezpieczenia oraz wdrażamy procedury i mechanizmy ochrony informacji, w tym system zarządzania bezpieczeństwem informacji. Wyniki analizy ataku wykorzystamy do dalszego wzmocnienia ochrony. Naszym priorytetem jest ograniczenie skutków zdarzenia, bezpieczne przywrócenie działania systemów i pomoc osobom, których dane mogły zostać objęte incydentem.

Stan ustaleń na dzień 3 listopada 2026

Element	Stan
Wykrycie ataku - 29 października 2026 r.	● Potwierdzone
Zaszyfrowanie danych i utrata dostępu do części zasobów	● Potwierdzone
Odczytanie lub skopiowanie danych przez sprawców	● W trakcie weryfikacji
Zakres danych, liczba osób i okres, którego dotyczą dane	● W trakcie weryfikacji
Zgłoszenie do Prezesa UODO, CSIRT i Policji	● Dokonane
Odtwarzanie danych z kopii zapasowych	● W toku

SKALA ZAGROŻEŃ W POLSCE

Według CERT Polska w 2025 r. zarejestrowano 260 783 incydenty bezpieczeństwa, a liczba odnotowanych incydentów ransomware wyniosła 179 - o 21% więcej niż rok wcześniej. Są to zdarzenia zarejestrowane przez CERT Polska, a nie wszystkie ataki w kraju. Nawet rozbudowane zabezpieczenia nie eliminują ryzyka całkowicie - nie zmienia to naszej odpowiedzialności za ochronę danych, wyjaśnienie zdarzenia i wsparcie Państwa.

05 Najczęściej zadawane pytania

Czy moje dane na pewno wyciekły?

Tego jeszcze nie wiemy. Potwierdzone jest zaszyfrowanie danych. Ustalamy, czy sprawcy je odczytali lub skopiowali - ponieważ nie możemy tego wykluczyć, zalecamy podjęcie działań ochronnych już teraz.

Czy zastrzeżenie PESEL jest płatne i ile trwa?

Jest bezpłatne i działa od razu. Nie blokuje przelewów, wypłat z bankomatu, wizyty u lekarza, realizacji recepty, wyjazdu za granicę ani załatwiania spraw urzędowych.

Planuję wziąć kredyt. Co wtedy?

Zastrzeżenie można w każdej chwili cofnąć - także czasowo, z automatycznym ponownym zastrzeżeniem w wybranym terminie. Cofnięcie najlepiej uzgodnić z bankiem przed podpisaniem umowy.

Czy mogę zastrzec PESEL dziecka?

Standardowa usługa jest przeznaczona dla osób pełnoletnich. W przypadku dzieci należy zachować szczególną ostrożność wobec prób wyłudzania danych i pieniędzy.

Czy Farmutil będzie się ze mną kontaktować?

Możemy kontaktować się w sprawach związanych z incydentem, ale nie poprosimy o hasła, kody autoryzacyjne, dane do bankowości ani o wykonanie przelewu. W razie wątpliwości prosimy zakończyć rozmowę i skontaktować się z punktem pomocy.

Doszło już do próby oszustwa. Co robić?

Należy natychmiast skontaktować się z bankiem, zgłosić sprawę Policji, zachować wszystkie dowody (wiadomości, numery, potwierdzenia) i poinformować punkt pomocy Spółki.

Gdzie znajdę aktualne informacje?

Kolejne istotne informacje będziemy publikować pod tym samym adresem i przekazywać bezpośrednio osobom, których dotyczą.

06 Gdzie uzyskać pomoc

Jeśli potrzebują Państwo wyjaśnień, pomocy w zastrzeżeniu PESEL lub chcą zgłosić podejrzany kontakt związany z incydentem, prosimy o kontakt:

OCHRONA DANYCH

Inspektor Ochrony Danych

Robert Erdmann

rodo@farmutil.pl

SPRAWY ORGANIZACYJNE

Punkt pomocy

Dział Personalny

Tel.: 782 971 125 I Dostępność w dni powszednie w godz. 7:00 – 15:00

BEZPIECZNY KONTAKT

Prosimy nie przesyłać zwykłą wiadomością e-mail skanu dokumentu tożsamości ani pełnego numeru PESEL. Jeżeli do wyjaśnienia sprawy potrzebna będzie weryfikacja tożsamości, uzgodnimy jej bezpieczny sposób.

Zakład Rolniczo-Przemysłowy „FARMUTIL HS" S.A.
ul. Przemysłowa 4, Śmiłowo, 64-810 Kaczory