POLISH WEBSITE NOTICE

17 listopada 2026 r.

KOMUNIKAT O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

CO SIĘ WYDARZYŁO?

W dniu 25 lipca 2026 r. WireCo World Group Inc. oraz jej spółki zależne („WireCo", „my" lub „nas") wykryły nieuprawnioną aktywność w swoich wewnętrznych systemach informatycznych, która – jak następnie ustaliliśmy – była cyberatakiem przeprowadzonym przez znanego i zaawansowanego technicznie sprawcę. Po wykryciu incydentu odizolowaliśmy systemy, których dotyczył i – pod kierunkiem doradców prawnych – zaangażowaliśmy zewnętrznych ekspertów ds. cyberbezpieczeństwa w celu przeprowadzenia kompleksowego przeglądu naszej sieci wewnętrznej oraz wsparcia w wyjaśnieniu okoliczności incydentu, jego opanowaniu oraz usunięciu skutków. Według dotychczasowych ustaleń nieuprawniona aktywność miała miejsce w okresie od 9 lipca 2026 r. do 25 lipca 2026 r. Po zabezpieczeniu naszych wewnętrznych systemów informatycznych ustaliliśmy, że sprawca uzyskał dostęp do części danych zawierających dane osobowe i wykradł je z naszych systemów. Od chwili wykrycia ataku nieprzerwanie analizujemy dane objęte incydentem w celu zidentyfikowania znajdujących się w nich danych osobowych. Proces ten wymagał czasu.

JAKICH DANYCH OSOBOWYCH DOTYCZY INCYDENT?

Incydent dotyczył danych osobowych przechowywanych przez WireCo, które mogą obejmować:

- imiona i nazwiska oraz dane kontaktowe (adresy zamieszkania, numery telefonów, adresy e-mail);
- numery PESEL, inne krajowe numery identyfikacyjne lub numery ubezpieczenia społecznego;
- kopie paszportów lub innych urzędowych dokumentów tożsamości;
- daty urodzenia;
- informacje dotyczące rachunków bankowych i kart kredytowych.

Jeżeli byli Państwo pracownikami WireCo lub wykonywali Państwo pracę na rzecz WireCo, dane te mogą obejmować również:

- dokumentację pracowniczą, w tym oceny okresowe, informacje o postępowaniach dyscyplinarnych, przynależności do związków zawodowych i karalności;
- dane dotyczące nieobecności i stanu zdrowia (np. dokumentację zwolnień lekarskich oraz informacje z zakresu medycyny pracy);
- dane najbliższych członków rodziny oraz osób wskazanych do kontaktu w nagłych wypadkach.

JAKIE SĄ MOŻLIWE KONSEKWENCJE?

Ze względu na charakter danych objętych incydentem istnieje ryzyko narażenia Państwa na:

- kradzież tożsamości lub podszywanie się pod Państwa w celu dokonania oszustwa;

- próby phishingu (fałszywe wiadomości e-mail lub inne wiadomości mające na celu wyłudzenie dalszych danych osobowych);
- oszustwa finansowe, w szczególności w razie nieuprawnionego wykorzystania danych bankowych, numerów PESEL lub numerów ubezpieczenia społecznego;
- niepożądane kontakty lub próby manipulacji socjotechnicznej.

Chcemy otwarcie poinformować Państwa o tych zagrożeniach, aby mogli Państwo podjąć odpowiednie kroki w celu własnej ochrony.

PODJĘTE PRZEZ NAS DZIAŁANIA

Przed wystąpieniem incydentu stosowaliśmy wielopoziomowy program cyberbezpieczeństwa obejmujący administracyjne, techniczne i organizacyjne środki bezpieczeństwa, mające na celu ograniczenie prawdopodobieństwa wystąpienia cyberzagrożeń i ich skutków oraz ochronę poufności, integralności i dostępności naszych systemów informatycznych i danych.

Od 25 lipca 2026 r. podjęliśmy szereg działań w celu dalszego wzmocnienia naszego programu cyberbezpieczeństwa oraz reakcji na incydent. W szczególności:

- odizolowaliśmy i zabezpieczyliśmy systemy objęte incydentem, aby zapobiec dalszemu nieuprawnionemu dostępowi;
- zaangażowaliśmy czołowych specjalistów ds. cyberbezpieczeństwa w celu przeprowadzenia analizy powłamaniowej;
- zgłosiliśmy incydent krajowym i lokalnym organom ochrony danych;
- przywróciliśmy zaszyfrowane systemy z bezpiecznych kopii zapasowych;
- wdrożyliśmy wzmocnione zabezpieczenia, w tym dodatkowy monitoring oraz ograniczenia dostępu do naszych systemów informatycznych;
- rozpoczęliśmy gruntowny przegląd naszych środków bezpieczeństwa informacji, aby zapobiec podobnym zdarzeniom w przyszłości.

Zleciliśmy również podmiotowi zewnętrznemu monitorowanie sieci dark web w celu ustalenia, czy dane z naszych systemów zostały w niej udostępnione. Chociaż sprawca opublikował link do plików objętych incydentem, do tej pory nie mamy żadnych informacji wskazujących na to, że jakiekolwiek dane osobowe zostały sprzedane lub wystawione na sprzedaż, ani dowodów na dalsze niewłaściwe wykorzystanie tych danych.

Obecni pracownicy WireCo zostali już poinformowani o incydencie. Nie dysponujemy jednak danymi kontaktowymi niewielkiej liczby byłych pracowników, klientów, dostawców i osób odwiedzających nasze obiekty. Dlatego publikujemy niniejszy komunikat, aby poinformować o incydencie osoby, z którymi nie możemy skontaktować się bezpośrednio.

CO MOGĄ PAŃSTWO ZROBIĆ

Chociaż nie są nam znane żadne przypadki oszustw ani prób oszustw związanych z niewłaściwym wykorzystaniem danych osobowych ani szkody finansowe poniesione w wyniku tego incydentu przez osoby, których dane dotyczą, zalecamy podjęcie następujących środków ostrożności:

- **Monitorowanie rachunków bankowych i raportów kredytowych (np. raportu BIK)** – prosimy zwracać uwagę na wszelkie nietypowe lub nieautoryzowane transakcje i niezwłocznie zgłaszać je swojemu bankowi.

- **Zastrzeżenie numeru PESEL** – zalecamy zastrzeżenie numeru PESEL, co można zrobić bezpłatnie m.in. w aplikacji mObywatel, w serwisie gov.pl lub w urzędzie gminy. Zastrzeżenie utrudnia osobom trzecim posłużenie się Państwa numerem PESEL, np. w celu zaciągnięcia kredytu lub pożyczki na Państwa dane.
- **Zachowanie czujności wobec phishingu** – prosimy zachować ostrożność w przypadku nieoczekiwanych wiadomości e-mail, SMS-ów lub połączeń telefonicznych z prośbą o podanie danych osobowych, nawet jeśli wydają się one pochodzić z zaufanego źródła.
- **Zmiana haseł** – zalecamy zmianę haseł do kont prywatnych, zwłaszcza jeśli mogli Państwo używać haseł podobnych do tych stosowanych w systemach służbowych.

Jak zawsze zachęcamy Państwa do zachowania czujności wobec prób kradzieży tożsamości i oszustw, sprawdzania wyciągów z rachunków oraz monitorowania bezpłatnych raportów kredytowych pod kątem podejrzanej aktywności i ewentualnych błędów.

PAŃSTWA PRAWA

Przepisy o ochronie danych osobowych przyznają określone prawa w związku z przetwarzaniem danych osobowych. Zakres przysługujących praw zależy od jurysdykcji i może obejmować prawo dostępu do danych, prawo do ich sprostowania oraz – w określonych przypadkach – prawo do ich usunięcia. Jeżeli chcą Państwo skorzystać z któregokolwiek z tych praw, prosimy o przesłanie wniosku w formie pisemnej lub elektronicznej z wykorzystaniem danych kontaktowych podanych poniżej.

DODATKOWE INFORMACJE

Wiemy, że powierzają nam Państwo ważne informacje, i zapewniamy, że traktujemy ten incydent oraz bezpieczeństwo i ochronę Państwa danych osobowych z pełną powagą. Szczerze ubolewamy, że do niego doszło. W razie jakichkolwiek pytań lub wątpliwości prosimy o kontakt z Dan Burch pod adresem DanBurch@WireCo.com.

Informacje o administratorach danych

JURYSDYKCJA	ADMINISTRATOR DANYCH
Dania	**Euronete Scandinavia A/S** **Adres:** Gothersgade 48, 7000 Fredericia, Dania
Francja	**Le Drezen SAS** **Adres:** 12 rue de Kelareun, 29730 Guilvinec-Treffiagat, Francja
Niemcy	**WireCo Germany GmbH** **Adres:** Casarstraße 1, 66459 Kirkel-Limbach, Niemcy
Holandia	**Lankhorst Engineered Products B.V.** **Adres:** Prinsengracht 2, 8607AD, Sneek, Holandia **Ekon B.V.** **Adres:** Holtum-Noordweg 8, 6121 RE Born, Holandia **Lankhorst Touwfabrieken B.V.** **Adres:** Marconiweg 24, 3316 AM Dordrecht, Holandia **Royal Lankhorst-Euronete group B.V.** **Adres:** Prinsengracht 2, 8607AD, Sneek, Holandia
Polska	**WireCo Poland sp. z o.o.** **Adres:** ul. Polna 26/74, 87-806 Włocławek, Polska
Portugalia	**Oliveira Sá, S.A.** **Adres:** Rua Do Outeiro, 906, 4475-150, Maia, Portugalia **Lankhorst Euronete Portugal, S.A.** **Adres:** Rua da Cerfil , (Cap.Gramaxo) nº45, 4475-468, Maia, Portugalia
Wielka Brytania	**Euronete (UK) Limited** **Adres:** Enerfield Business Park, Foveran, Ellon, Newburgh Aberdeenshire, AB41 6AL, Wielka Brytania
Brazylia	**WireCo do Brasil Ltda** **Adres:** Rua Minas Gerais 1920, Distrito Industrial Queimados, Rio de Janeiro, Brazylia **Lankhorst-Euronete (Brasil) –Indústria e Comércio Ltda**

	Adres: Rua Minas Gerais 1920, Distrito Industrial Queimados, Rio de Janeiro, Brazylia
Meksyk	**Aceros Camesa S.A. de C.V.** **Adres:** Margarita Maza de Juarez 159, Nueva Industrial Vallejo, Gustavo A. Madero, Mexico City 07700
Australia	**WireCo Australia Pty Ltd** **Adres:** 7 Demand Avenue, Arundel QLD 4214, Australia