Wiceprezes Rady Ministrów
Minister Cyfryzacji

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Krzysztof Gawkowski

$znak pisma
Warszawa, 12 września 2025 r.

KOMUNIKAT
Pełnomocnika Rządu do spraw Cyberbezpieczeństwa
w sprawie wycieku danych w wyniku cyberataku wobec firmy
EKOTRADE Sp. z o.o

Informuję o utrzymującym się dużym poziomie ryzyka wystąpienia incydentów w polskiej cyberprzestrzeni. Do najbardziej destrukcyjnych ataków należą ataki ransomware prowadzące do wycieków danych. Jednym z najnowszych przypadków, jest cyberatak dokonany wobec firmy **EKOTRADE Sp. z o.o.** z siedzibą w Warszawie (KRS: 0000020453).

Wyciek danych po ataku na firmę EKOTRADE Sp. z o.o.:

Na podstawie analizy Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) poziomu krajowego[1] stwierdza się, iż omawiany incydent miał miejsce 31 sierpnia 2025 r. Przedmiotem ataku była infrastruktura IT, w której znajdowała się m.in. baza informacji kadrowo-płacowych dotyczących pracowników firmy. Zgodnie z komunikatem firmy Ekotrade[2] oraz analizą krajowych zespołów CSIRT wykradzione dane mogą obejmować:

- dane osobowe,
- zawarte umowy,
- informacje o realizowanych przetargach,
- zawartość skrzynek pocztowych pracowników i baz danych firmy,
- dane dostępowe do kont serwisowych u klientów,
- specyfikacje techniczne projektów,
- inne wrażliwe informacje.

Zalecenia Pełnomocnika Rządu do spraw Cyberbezpieczeństwa:

Aby zminimalizować skutki ataku i zapobiec dalszym zagrożeniom, rekomenduję następujące działania:

- Weryfikacja danych udostępnianych w komunikacji z firmą Ekotrade i podjęcie kroków prewencyjnych w wypadku stwierdzenia udostępnienia danych wrażliwych, np. danych dostępowych do systemów organizacji.
- Zablokowanie zdalnego dostępu do kont serwisowych udostępnionych firmie Ekotrade oraz połączeń VPN z firmy Ekotrade. Ważnym jest uniemożliwienie potencjalnego nieuprawnionego dostępu do tych kont.
- Analiza logów co najmniej od 1 sierpnia 2025 r. Szczególną uwagę należy zwrócić na logi systemowe, aby wykryć możliwe przypadki nieuprawnionego

[1] Ustawa z dnia z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077, z późn. zm.)
[2] Komunikat Ekotrade Sp. z o. o. dot. ataku na infrastrukturę informatyczną spółki.

telefon: +48 22 245 59 22
adres email: sekretariat.dc@cyfra.gov.pl
www.gov.pl/cyfryzacja

ul. Królewska 27
00-060 Warszawa

użycia kont serwisowych lub innych nadużyć wynikających z dostępu atakujących do danych Ekotrade.
- Zmiana poświadczeń do wszystkich kont i systemów związanych z Ekotrade.
- Wdrożenie dwuskładnikowego uwierzytelniania dla kont serwisowych, w szczególności dla usług zdalnego dostępu.
- Monitorowanie kampanii socjotechnicznych, które wykorzystują wizerunek Ekotrade.
- Zachowanie wzmożonej czujności wobec prób wyłudzania informacji, które mogą wykorzystywać nazwę firmy.
- Zgłaszanie incydentów do odpowiednich zespołów CSIRT. Każdy potencjalny incydent powinien być bezzwłocznie zgłoszony do odpowiedniego CSIRT-u.

Dodatkowe środki bezpieczeństwa:

Zwracam szczególną uwagę na konieczność podjęcia działań prewencyjnych, celem zmniejszenia ryzyka przyszłych incydentów. Wśród nich zaleca się:

- Stosować dwuskładnikowe uwierzytelnianie z wykorzystaniem kluczy sprzętowych, szczególnie dla kont serwisowych i z uprawnieniami administratora.
- Stosować menedżery haseł do bezpiecznego przechowywania danych uwierzytelniających.
- Regularnie aktualizować oprogramowanie, zwłaszcza w systemach związanych z dostępem do sieci Internet.
- Stosować segmentację sieci celem podniesienia bezpieczeństwa wrażliwych elementów infrastruktury.

Implementacja ww. zaleceń jest również zasadna w przypadku podobnych incydentów w innych podmiotach, z którymi została nawiązana współpraca.

Krzysztof Gawkowski
Wiceprezes Rady Ministrów
Minister Cyfryzacji
/dokument podpisany elektronicznie/

telefon: +48 22 245 59 22
adres email: sekretariat.dc@cyfra.gov.pl
www.gov.pl/cyfryzacja
ul. Królewska 27
00-060 Warszawa