Wiceprezes Rady Ministrów
Minister Cyfryzacji

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Krzysztof Gawkowski

Warszawa, 17.01.2025 r.

KOMUNIKAT
Pełnomocnika Rządu do spraw Cyberbezpieczeństwa
ws. wycieku danych w wyniku cyberataku wobec firmy
EUROCERT Sp. z o.o.:

Pełnomocnik Rządu do spraw Cyberbezpieczeństwa, Krzysztof Gawkowski, informuje 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 EUROCERT Sp. z o.o. - dostawcę kwalifikowanych i niekwalifikowanych usług zaufania.

Wyciek danych po ataku na firmę EUROCERT Sp. z o.o.:
W ramach posiedzenia Połączonego Centrum Operacyjnego Cyberbezpieczeństwa ustalono, że wykradzione dane mogą obejmować:

- dane osobowe,
- zawarte umowy,
- informacje o realizowanych przedsięwzięciach,
- dane dostępowe,
- inne wrażliwe informacje.

Trwa analiza, która jest prowadzona przez CSIRT NASK. Współpracują z nimi Centralne Biuro Zwalczania Cyberprzestępczości, inne krajowe CSIRT-y oraz Ministerstwo Cyfryzacji. Celem podsumowania wyników przedmiotowej analizy oraz podjęcia dalszych działań naprawczych zwołane zostało posiedzenie Zespołu do spraw Incydentów Krytycznych.

Zalecenia Pełnomocnika Rządu do spraw Cyberbezpieczeństwa:
Aby zminimalizować skutki ataku i zapobiec dalszym zagrożeniom, Pełnomocnik Rządu do spraw Cyberbezpieczeństwa rekomenduje następujące działania:

1. **Przegląd infrastruktury.**
   Należy przeanalizować dane przetwarzane oraz rozwiązane udostępniane przez EUROCERT, aby zidentyfikować możliwe cyberataki na obecnych i byłych kontrahentów.
2. **Zablokowanie zdalnego dostępu i powiązań infrastruktury IT z EUROCERT.**
   Ważne jest, aby uniemożliwić potencjalny nieuprawniony dostęp do własnej infrastruktury.

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

ul. Królewska 27
00-060 Warszawa

3. **Analiza logów od dnia 1 listopada 2024 r.**
   Należy sprawdzić logi systemowe, aby wykryć możliwe przypadki nieuprawnionego użycia powiązań międzysystemowych czy kont serwisowych.
4. **Zmiana poświadczeń do wszystkich kont i systemów związanych z EUROCERT.**
   Trzeba zaktualizować wszystkie dane logowania.
5. **Wdrożenie dwuskładnikowego uwierzytelniania dla kont zewnętrznych.**
   Należy wprowadzić dodatkowe zabezpieczenia w postaci dwuskładnikowego uwierzytelniania.
6. **Monitorowanie kampanii socjotechnicznych, które wykorzystują wizerunek EUROCERT.**
   Zaleca się wzmożoną czujność wobec prób wyłudzania informacji, które mogą wykorzystywać nazwę firmy w tym podszywające się pod informację o wycieku danych.
7. **Przeprowadzenie analizy ryzyka korzystania z podpisów kwalifikowanych oraz pieczęci dostarczanych przez EUROCERT.**
   Należy przeanalizować możliwość nieuprawnionego wykorzystania usług zaufania dostarczonych przez EUROCERT oraz nieuprawnionego wykorzystania danych osobowych posiadanych przez EUROCERT**, w szczególności w podmiotach administracji publicznej**.
8. **Zgłaszanie incydentów do odpowiednich zespołów CSIRT.**
   Każdy podejrzany incydent powinien być bezzwłocznie zgłoszony do odpowiedniego CSIRT-u.

Dodatkowe środki bezpieczeństwa:
Pełnomocnik Rządu do spraw Cyberbezpieczeństwa zwraca również uwagę na kluczowe działania prewencyjne, aby zmniejszyć ryzyko przyszłych incydentów. Wśród nich zaleca się:

- Stosować dwuskładnikowe uwierzytelnianie, szczególnie dla kont serwisowych.
- Regularnie aktualizować oprogramowanie, zwłaszcza w systemach związanych z dostępem do Internetu.

Te zalecenia są również przydatne w przypadku podobnych incydentów w innych podmiotach, z którymi współpracujemy.