

„Harvest now, decrypt later"

keep it cyber-safe

Hakerzy z przyszłości?



Cyberatak, który zaczyna się dziś a kończy za 10 lat

Czy wiesz o tym, że cyberprzestępcy już dziś mogą gromadzić zaszyfrowane dane, aby odczytać je dopiero za kilka lat?

Europol ostrzega przed nowym rodzajem cyberzagrożeń.

Wyobraź sobie, że ktoś przechwytuje Twoją poufną korespondencję, ale nie potrafi jej odczytać, bo chroni ją silne szyfrowanie. Jednak zamiast bezskutecznie próbować je złamać, zapisuje te dane i cierpliwie czeka.



„Harvest now, decrypt later"

To strategia polegająca na pozyskiwaniu i przechowywaniu zaszyfrowanych danych z zamiarem ich odszyfrowania w przyszłości, gdy pozwoli na to rozwój technologii.

W październiku 2026 r. Europol (Agencja Unii Europejskiej ds. Współpracy Organów Ścigania) opublikował raport poświęcony temu zagrożeniu.

Wskazuje w nim, że rozwój komputerów kwantowych może w przyszłości umożliwić złamanie części powszechnie stosowanych zabezpieczeń kryptograficznych.

Dlaczego to problem już teraz?

Wiele informacji nie traci na wartości z upływem kilku miesięcy czy lat.

Na przykład dokumentacja medyczna, tajemnice przedsiębiorstwa czy własność intelektualna mogą wymagać ochrony przez o wiele dłuższy czas.

Pokazują to też ostatnie naruszenia ochrony danych, o których było głośno w Polsce.

W przypadku danych o długotrwałej wartości skutki ich wycieku mogą wykraczać daleko poza moment samego cyberataku.



Co to oznacza w praktyce?

Przede wszystkim warto przyjrzeć się:

- jakie informacje przetwarza nasza organizacja
- jak długo powinny pozostać poufne
- w jaki sposób są zabezpieczane.

Szczególnej uwagi wymagają dane, których ujawnienie nawet za kilka lub kilkanaście lat mogłoby wyrządzić poważne szkody.

Co radzi Europol?

Europol w swoim raporcie radzi, aby zadbać o aktualność stosowanych zabezpieczeń.

W praktyce oznacza to między innymi korzystanie z nowoczesnych protokołów bezpieczeństwa (np. TLS 1.3 i SSH2), rezygnację z przestarzałych rozwiązań oraz regularne aktualizowanie oprogramowania. Ważne jest też ograniczenie przechowywania poufnych danych, które nie są już potrzebne.

W dłuższej perspektywie należy przygotowywać się do wdrażania kryptografii postkwantowej, czyli rozwiązań odpornych na zagrożenia związane z rozwojem komputerów kwantowych.

Nowe technologie otwierają nowe możliwości, również przed cyberprzestępcami.

Dlatego warto myśleć o bezpieczeństwie danych nie tylko z perspektywy dzisiejszych zagrożeń.

Pełną treść raportu Europolu znajdziesz tutaj

Potrzebujesz więcej informacji?
Zapraszamy do kontaktu!

Agnieszka Witaszek



agnieszka.witaszek
@ssw.solutions

Martyna Taciak-Jankowiak



martyna.taciak
@ssw.solutions