EUROPEJSKI MIESIĄC CYBER BEZPIECZEŃSTWA

Zagrożenia i cyberataki w trakcie wakcji

Czy wiesz, że...

Oszustwa komputerowe stanowią największą liczbę - ok. 76 tysięcy – zarejestrowanych przez CERT Polska tego typu incydentów w 2023 roku*

*Źródło: Raport roczny z działalności CERT Polska 2023

Socjotechnika

Większość cyberprzestępstw opiera się na **socjotechnice**. To wszelkie formy manipulacji i techniki psychologiczne, których celem jest skłonienie ludzi do określonych działań, które często prowadzą do ujawnienia poufnych informacji, utraty danych, a w konsekwencji także środków finansowych.

Najpopularniejsze zagrożenia

- **Phishing** - oszustwo polegające na podszywaniu się pod zaufane osoby, firmy lub instytucje, wykorzystując w tym celu m.in. wiadomości e-mail, SMS, komunikatory
- **Ataki typu BEC** (*z ang. Business Email Compromise*) to oszustwa, w których cyberprzestepcy podszywają się pod pracowników wysokiego szczebla firmy, aby nakłonić innych pracowników do wykonania nieautoryzowanych przelewów finansowych lub ujawnienia wrażliwych informacji.
- **Ransomware -** to złośliwe oprogramowanie, które infekuje i blokuje system komputerowy, szyfrując wybrane pliki w celu wyłudzenia okupu.

Jak się chronić?

- Regularnie przeprowadzaj szkolenia i warsztaty zwiększające kompetencje pracowników.
- Zapewnij bezpieczeństwo systemów poprzez regularne i automatyczne aktualizacje.
- Stosuj silne hasła do wszystkich usług.
- Włącz weryfikację dwuetapową na kontach online.
- Zawsze weryfikuj nadawcę wiadomości. Kontaktuj się bezpośrednio z osobą, która zleca Ci zadania (np. telefonicznie).
- Unikaj otwierania załączników lub linków z nieznanych źródeł.
- Regularnie twórz kopie zapasowe danych.
- Weryfikuj żądania zmiany numeru konta i potwierdzaj transakcje finansowe.