CSIRT CEZ

Ochrona przed atakami socjotechnicznymi

w ramach zaleceń w zakresie podstaw bezpieczeństwa i ochrony danych dla użytkowników w sektorze ochrony zdrowia

01. Jak rozpoznać próbę ataku socjotechnicznego? Jak działają cyberprzestępcy?

- Wykorzystują presję czasu oraz pilność działania, twierdząc, że musisz natychmiast wykonać przelew, zmienić hasło lub przekazać dane logowania, strasząc konsekwencjami.
- Podszywają się pod przełożonych, pracowników działów IT, dostawców usług, banki lub instytucje rządowe, aby wzbudzić Twoje zaufanie.
- Próbują zdobyć Twoją sympatię lub wzbudzić strach, by zmusić Cię do działania.
- Dzwonią z nieznanych lub ukrytych numerów telefonów oraz wykorzystują fałszywe (chociaż z pozoru poprawne) adresy e-mail.
- Proszą o podanie poufnych danych, zwykle posiadając już wcześniej pewne dane ofiary np. adres zamieszkania, nazwisko przełożonego bądź prywatny nr telefonu.
- Alarmujące powinno być nieoczekiwane powiadomienie o logowaniu lub próbie dostępu, którego nie wykonałeś.
- Możesz otrzymać informację o fałszywej sytuacji kryzysowej (np. „Twoje konto zostało zhakowane, musisz natychmiast zmienić hasło" lub „Twoja firma została zaatakowana, pobierz to narzędzie do zabezpieczenia systemu").
- Wykorzystują nietypowe sposoby komunikacji np. „przełożony" nagle pisze do Ciebie przez prywatny adres e-mail lub komunikator, zamiast przez firmowe kanały komunikacji.

CSIRT CEZ

02. Jak zapobiegać atakom socjotechnicznym?

- Nie podejmuj żadnych działań pod presją. Jeśli rozmówca nalega na szybkie działanie, wstrzymaj się i sprawdź sytuację.
- Weryfikuj rozmówców, zanim przekażesz jakiekolwiek informacje. Zawsze sprawdzaj tożsamość osób, które proszą o dostęp do danych lub systemów.
- Jeśli przełożony lub pracownik działu IT prosi Cię o zmianę hasła, przelew lub dostęp do systemu, potwierdź to innym kanałem.
- Korzystaj z uwierzytelniania wieloskładnikowego (MFA).
- Konsultuj się ze współpracownikami, jeśli coś budzi Twój niepokój.
- Zgłaszaj wszelkie podejrzane sytuacje do odpowiedniego działu (bezpieczeństwa lub IT).
- Nie udostępniaj w mediach społecznościowych informacji o pracy i strukturze firmy. Oszuści mogą wykorzystać takie dane do przygotowania przekonujących ataków.
- Ogranicz dostęp do poufnych informacji. Niech będą dostępne tylko dla upoważnionych osób.
- Unikaj dzielenia się informacjami przez niezabezpieczone kanały komunikacji. Do przesyłania poufnych danych używaj tylko autoryzowanych systemów firmowych.
- Stosuj zasadę minimalnych uprawnień oraz nie udostępniaj danych osobom spoza firmy.
- Nie otwieraj podejrzanych linków i załączników w e-mailach. Nawet jeśli wiadomość pochodzi od znanego nadawcy, sprawdź jej autentyczność.
- Nie pobieraj i nie instaluj oprogramowania spoza oficjalnych źródeł.Cyberprzestępcy mogą zachęcać do instalacji „aktualizacji” lub „narzędzi bezpieczeństwa”, które w rzeczywistości zawierają złośliwe oprogramowanie.

CSIRT CEZ