Atak typu Buisness E-mail Compromise

ATAK TYPU BUISNESS E-MAIL COMPROMISE (BEC) – znany również jako „oszustwo na dyrektora", to oszustwo z użyciem socjotechniki, w którym cyberprzestępcy wykorzystują korespondencję e-mailową do wyłudzeń finansowych lub ujawniania poufnych danych firmowych.

Cyberprzestępca

1. Zbiera informacje o organizacji i jej pracownikach, zależnościach służbowych.
2. Przygotowuje i wysyła fałszywe wiadomości e-mail podszywając się pod osobę na kluczowym stanowisku.

Fałszywy e-mail

- Wiadomość do złudzenia przypomina prawdziwy e-mail.
- Wykorzystanie wizerunku przełożonego.
- Presja czasu, ponaglanie do działania.
- Prośba o zachowanie poufności.

Konsekwencje

- Przelew na konto cyberprzestępcy.
- Ujawnienie poufnych danych.
- Zainfekowanie urządzenia, zaszyfrowanie lub kradzież danych.

Odbiorca e-maila

Pracownik (np. uprawniony do wykonywania przelewów)

1. Otrzymuje fałszywy e-mail.
2. Podejmuje określone działania zgodnie z treścią fałszywego e-maila.
3. Wykonuje przelew na wskazane konto lub nieświadomie pobiera zainfekowany załącznik.

Jak się chronić?

1. **DOKŁADNIE ZWERYFIKUJ NADAWCĘ** wiadomości. Sprawdź adres e-mail oraz potwierdź tożsamość np. poprzez rozmowę telefoniczną.
2. **REGULARNIE AKTUALIZUJ SPRZĘT I OPROGRAMOWANIE,** z którego korzystasz.
3. **NIE KLIKAJ W LINKI I NIE POBIERAJ ZAŁĄCZNIKÓW,** jeśli nie masz pewności skąd podchodzą lub co zawierają.
4. **STOSUJ SIĘ DO PROCEDUR BEZPIECZEŃSTWA** w swojej organizacji, szczególnie tych związanych z płatnościami.
5. **NIGDY NIE DZIAŁAJ POD PRESJĄ CZASU LUB AUTORYTETU**, zawsze weryfikuj autentyczność polecenia.
6. **NIE PRZEKAZUJ INFORMACJI** na temat swojej organizacji osobom postronnym i nie udostępniaj ich w sieci.
7. **JEŚLI OTRZYMASZ NIETYPOWĄ WIADOMOŚĆ**, zgłoś ją do działu bezpieczeństwa lub IT w swojej organizacji.

NASK
EUROPEJSKI MIESIĄC CYBERBEZPIECZEŃSTWA
PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTRA CYFRYZACJI