

## O święta naiwności, czyli o magii nazwiska i stanowiska

Kilka dni temu złapano pewnego sprytnego złodzieja – przez blisko rok, w banalny sposób okradał firmy na kilkanaście tysięcy złotych każdą. Pieniądze dostawał niemal legalnie – przelewane na jego konto przez głównych księgowych tych firm – wystarczyło sprawdzić w internecie strukturę firmy, następnie założyć na darmowym portalu konto internetowe typu imie.nazwisko@ (podstawiając oczywiście dane odpowiedniego prezesa) i wysłać maila z wytycznymi dotyczącymi przelewu w trybie pilnym. Na kilkadziesiąt osób, które otrzymały takiego maila, nabrało się ponad trzydzieści – 30 osób z doświadczeniem w swoim zawodzie, osób, które powinny mieć wyrobiony nawyk ograniczonego zaufania i wielokrotnego sprawdzania danych.

Na pewno nie mało pomógł złodziejowi Outlook Express, bardzo często wykorzystywany w firmach, a ukrywający (przynajmniej w podstawowych ustawieniach) adres nadawcy (pokazuje tylko to, co jest ustawione jako „nadawca” – najczęściej nazwisko lub ksywkę) – w tym momencie księgowi widzieli imię i nazwisko prezesa, a niemal na pewno nie zauważyli, że „prezes” nie wysłał im dyspozycji z adresu firmowego, tylko np. z „onetowego”, czy „gazetowego”. Niemniej jednak nie przyszło im do głowy sprawdzić czy takie zamówienie było złożone (w tytule przelewu były kaucje i zaliczki za laptopy i komputery), czy kiedykolwiek emailem otrzymali takie zlecenie – magia nazwiska prezesa (nierazko pewno niemal nieznanego osobiście) zadziałała bezbłędnie.

O takich, niemal automatycznych reakcjach na nazwisko prezesa firmy, a także np. na hasło „konsultant”, czy „administrator sieci”, czyli osób, które w naszym poczuciu mają prawo dostępu do pewnych danych, pisał Kevin Mitnick – jeden ze znanych amerykańskich hackerów, który znacznie częściej włamywał się do systemów nie za pomocą skomplikowanego oprogramowania, a telefonu i magii nazwisk i stanowisk. Bez trudu otrzymywał nazwiska ludzi zatrudnionych w danej firmie, mówiąc np. „jestem nowy, szef kazał mi się skontaktować, zgubiłem kartkę, proszę mi pomóc, to mój okres próbny” (tę metodę nierazko stosują dziś head hunterzy), hasła do kont pocztowych, czy komputerów firmowych („jestem administratorem, coś się tam u was dzieje, podejrzewamy wirusy – musimy przeskanować wasze komputery/sprawdzić wasze konta, proszę o hasło”), czy też wewnętrzne dokumenty („nazywam się XY (tu oczywiście nazwisko kogoś ważnego), mam awarię komputera, a bardzo pilnie potrzebuję wasz ostatni raport finansowy – proszę mi go przesłać na adres ... (tu podawał jakiś prywatny)).

Wydawałoby się, że nikt nie poda nazwisk, nie mówiąc o hasłach, czy też wysyłaniu wewnętrznych, często tajnych dokumentów, na nieznaną adres. A mimo to wiele osób bez wahania spełniało jego prośby, stając się otwartą bramą do systemu i firmy.

Oczywiście, najłatwiejszym sposobem obrony jest wprowadzenie w firmach ścisłych procedur, mimo to, dopóki sami przed sobą nie przyznamy się, że i nas działają takie sztuczki, że i my bez trudu podamy „nowej księgowej (z zewnętrznej firmy), która zgubiła kartkę” nazwisko szefa finansów, a „konsultantowi z centrali” prześlemy np. zestawienie na temat sprzedaży za ostatnie pół roku, dotąd żadne procedury i żadne zabezpieczenia nie będą nawet w 80% skuteczne, a kolejną ofiarą sprytnego złodziejaska (pieniędzy lub danych) możemy stać się sami.

Anna Watza