Cyberprzestępczość: „na wnuczka 2.0", czyli oszuści w rzeczywistości wirtualnej

Prowadzenie biznesu nie jest dziś możliwe bez stosowania nowych technologii, zwłaszcza w szeroko pojętej komunikacji. Okazuje się, że całkiem niespodziewanie użytkownik takich technologii może poczuć się jak bohater filmu. Niestety, nie zawsze kończącego się dobrze.

Jan Rysiński
Adwokat, senior associate w kancelarii Łaszczuk i Wspólnicy Sp.k.

Scenariusz pierwszy: do dyrektora spółki należącej do międzynarodowej korporacji dociera e-mail od szefa, samego prezesa holdingu. Jak wynika z e-maila, holding potrzebuje wsparcia w pilnej międzynarodowej transakcji. Już po chwili, lekko zdezorientowany dyrektor odbiera telefon od prezesa, polecającego pilnie skontaktować się z doradzającym przy transakcji prawnikiem, który ma udzielić instrukcji co do dalszych kroków. Jak się okazuje, w związku z transakcją trzeba szybko zrobić przelew na kilkaset tysięcy euro. Oczywiście spółka nie poniesie żadnych własnych kosztów, holding natychmiast zwróci całą sumę na jej rachunek.

Mija kilka dni. Zwrotny przelew nie dociera. Prezes i prawnik przestali odbierać telefony.

Scenariusz drugi: do księgowej w dużej spółce wynajmującej biuro w prestiżowej lokalizacji dociera e-mail od wynajmującego: zmienia się numer rachunku bankowego, na który trzeba będzie przelewać czynsz. Wkrótce potem do księgowej dzwoni przedstawiciel wynajmującego, uprzejmie upewniający się, czy informacja o zmianie rachunku dotarła do odpowiedniej osoby. Zgodnie z otrzymaną instrukcją księgowa przelewa na podany rachunek kilkadziesiąt tysięcy euro.

Mija kilka dni. Do spółki dzwoni wynajmujący, zdziwiony brakiem płatności czynszu za ostatni okres.

Zakończenie obu historii jest podobne. Dyrektor i księgowa dowiadują się, że w rzeczywistości nie było żadnej transakcji, a rachunek bankowy wynajmującego się nie zmienił. Z dyrektorem nie kontaktował się żaden prezes, a z księgową wynajmujący. Zostali oszukani.

Dopiero wtedy oboje orientują się, że e-maile, choć graficznie są nie do odróżnienia od oryginalnych (czcionka, stopka, logotypy, nawet disclaimer), przesyłane były w rzeczywistości z innych adresów niż te, które pokazują się odbiorcy. Takie dane widoczne są jednak dopiero po sprawdzeniu „właściwości" e-maila, czego nie robi nikt niemający wątpliwości, kto jest nadawcą (i mało kto spośród mających takie wątpliwości).

Choć obie historie przypominają scenariusz filmu kryminalnego, media raz po raz informują o kolejnych zupełnie realnych przypadkach podobnych ataków, w wyniku których firmy w całej Europie, w tym w Polsce, a także w USA, tracą ogromne kwoty, trafiające na konta międzynarodowych grup przestępczych.

W największych sprawach przestępcy starannie przygotowują atak, uprzednio badając ofiarę: jej organizację, kluczowe osoby, specyfikę pracy. Zagrożenie dotyka jednak firm niezależnie od wielkości czy branży. Ataki mogą dotyczyć znacznie mniejszych kwot i nie musi poprzedzać ich makiaweliczne rozpracowanie.

Niekiedy bardziej dotkliwe od utraty dużej kwoty może dla firmy okazać się ujawnienie poufnych danych i mogąca się z tym wiązać utrata renomy. Prawdziwą plagą są aktualnie konie trojańskie i wirusy przesyłane w e-mailach udających korespondencję od klientów lub dostawców usług, a nawet współpracowników czy firmowych urządzeń (np. skanerów).

Warto też pamiętać, że niekiedy bardziej dotkliwe od utraty dużej kwoty może dla firmy okazać się ujawnienie poufnych danych i mogąca się z tym wiązać utrata renomy. Prawdziwą plagą są aktualnie konie trojańskie i wirusy przesyłane w e-mailach udających korespondencję od klientów lub dostawców usług, a nawet współpracowników czy firmowych urządzeń (np. skanerów). Ataki takie mogą nie tylko wyrządzić poważne szkody w firmowym systemie informatycznym, ale także doprowadzić do wycieku tajemnic przedsiębiorstwa.

W wyniku ataków cyberprzestępców firmy w całej Europie, w tym w Polsce, a także w USA, tracą ogromne kwoty, trafiające na konta międzynarodowych grup przestępczych.

Po fakcie najłatwiej powiedzieć: „zawiódł człowiek". W żaden sposób nie poprawia to jednak niczyjego bezpieczeństwa. Jak zatem zabezpieczyć się przed zagrożeniem?

Kluczem do uniknięcia niepożądanych przygód wydaje się świadomość tego, co może się stać. Rozsądny przedsiębiorca powinien przede wszystkim intensywnie szkolić pracowników, uzmysławiając im potencjalne zagrożenia. Niezbędne jest dziś także wprowadzanie procedur bezpieczeństwa, dotyczących zwłaszcza obchodzenia się z korespondencją elektroniczną. Nawet najprostsza rada, w rodzaju „nie otwieraj załączników z podejrzanych maili", jest w stanie sprawić, że nie będzie trzeba zastanawiać się, czy zawiódł człowiek i czy na końcu czeka nas happy end.