**Jedno kliknięcie może cię kosztować 5 mln dolarów**

* **Błąd ludzki to powód największych strat, ponoszonych przez firmy na skutek cyberataku. W 2021 roku organizacje na całym świecie straciły średnio ponad 5 mln dolarów w wyniku ataków Business Email Compromise (BEC).**
* **Jednym z najgłośniejszych w ostatnich latach był atak na Toyotę, która straciła w ten sposób 37 mln dolarów. Jednak kradzież nawet z pozoru niewielkiej kwoty może wpędzić firmę w poważne kłopoty.**
* **Jednym ze sposobów na obronę przed manipulacjami hakerów są szkolenia pracowników w zakresie cyberbezpieczeństwa.**

Business Email Compromise (BEC) to wyrafinowana metoda cyberataku. Hakerzy podszywają się pod konkretne osoby zatrudnione w firmie, wysyłając w ich imieniu fałszywe wiadomości z prośbą o zmianę w metodzie płatności wraz z podaniem „nowego” numeru konta. Takie maile trafiają najczęściej do księgowych lub osób zajmujących wysokie pozycje w działach finansowych. Co się dzieje później – można już sobie wyobrazić. Według danych IBM, w 2021 roku ataki BEC okazały się najkosztowniejsze spośród wszystkich cyberataków, jakie skierowano na organizacje na całym świecie – „kosztowały” średnio 5 mln dolarów.[[1]](#footnote-1)

– *BEC nie są jednak najczęściej stosowaną metodą ataku, choć najkosztowniejszą dla firm. Tu nadal króluje phishing, który jest „wstępem” do ataku BEC. Zanim cyberprzestępca podszyje się pod przedstawiciela firmy lub kontrahenta ofiary, musi wcześniej w jakiś sposób zdobyć ich dane. Najczęściej w tym celu rozsyła zainfekowane linki w fałszywych wiadomościach lub wykonuje fałszywe połączenia telefoniczne do pracowników firmy w celu wyłudzenia dostępu do potrzebnych mu informacji. Hakerzy są podstępni, dlatego warto uodpornić pracowników na takie manipulacje. W tym celu warto przeprowadzać cykliczne szkolenia z zakresu cyberbezpieczeństwa. Dodam, że przestępcy chętnie atakują osoby pracujące na szeregowych stanowiskach* – mówi Patrycja Tatara ekspert ds. cyberbezpieczeństwa w Sprint S.A.

Phishing był najpopularniejszym rodzajem cyberataków również w Polsce. Stanowił niemal 77% wszystkich incydentów, obsłużonych przez CERT Polska. Liczba tego typu zdarzeń wzrosła o 196% r/r. W 2021 CERT odnotował aż 22 575 incydentów. To wystarczy, aby zorganizować atak BEC i narazić firmę na gigantyczne straty. Spójrzmy na najgłośniejsze przykłady z kraju i ze świata.

* **Atak na spółkę Cenzin (Polska Grupa Zbrojeniowa) – strata 4 mln zł**

Pod koniec 2018 roku hakerzy zaatakowali spółkę Cenzin, związaną z Polską Grupą Zbrojeniową. Cyberprzestępcy zastosowali BEC, podszywając się pod czeskiego kontrahenta. Wysyłali fałszywą wiadomość do polskiej organizacji z informacją o zmianie konta i prośbą o przesyłanie środków na „nowy”, wskazany w mailu rachunek bankowy. Osoby odpowiedzialne za finanse w polskiej spółce dokonały stosownych zmian w systemie płatności i kwoty za towar od czeskiego producenta przelewano na konto przestępców. W ten sposób firma straciła łącznie 4 mln złotych.

* **Toyota i 37 mln dolarów straty na skutek BEC**

Hakerzy atakują firmy różnej wielkości, w także działające globalnie. W 2019 roku ofiarą ataku BEC została Toyota Boshoku Corporation (producent części do samochodów koncernu Toyoty). Scenariusz był niemal identyczny, jak w przykładzie z Polski. Hakerzy podszyli się pod kontrahenta z zagranicy i wysłali fałszywą wiadomość do pracowników działu finansowo-księgowego, aby przelano kwotę na „nowe” konto. W ten sposób Toyota straciła 37 mln dolarów.

* **FACC – strata 42 mln euro**

Jeszcze większe straty zaliczyła kilka lat wcześniej Fischer Advanced Composite Components AG (FACC). Austriacki producent ultralekkich komponentów dla branży lotniczej, w 2016 roku również padł ofiarą ataku BEC. Tym razem pracownik działu finansowego otrzymał fałszywego maila, wysłanego w imieniu prezesa. Wiadomość zawierała polecenie zmiany danych kontrahenta. W efekcie firma przelała 42 mln euro na konto hakerów.

*– Te przykłady pokazują, że cyberataki mogą dotyczyć każdego. Wszyscy jesteśmy ludźmi i popełniamy błędy, z czego cyberprzestępcy doskonale zdają sobie sprawę. Hakerzy atakują zatem nie tylko duże przedsiębiorstwa, ale także sektor małych i średnich firm, a nawet organizacje non-profit. Przytoczę chociażby przykład z ubiegłego roku, kiedy ofiarą ataku BEC padł Philabundance, czyli non-profit bank żywności. Hakerzy podali się wówczas za firmę budowlaną, zajmującą się wznoszeniem budynku kuchni społecznej, mającego służyć tej organizacji. W ten sposób ukradli 923 533 dolarów. Choć nie jest to aż tak wysoka kwota, jak w przypadku opisanych wyżej przypadków, to pamiętajmy o efekcie skali. Czasem kradzież „raptem” kilkudziesięciu czy kilkunastu tysięcy może wpędzić firmę w poważne kłopoty finansowe –* dodaje Patrycja Tatara ze Sprint S.A.

**Każdy jest pracownikiem działu IT**

Obecnie trudno wskazać firmę, która działa bez dostępu do internetu i każdy pracownik może stać się ofiarą ataku hakerskiego. Wiedza na temat cyberzagrożeń powinna więc dotyczyć nie tylko zespołu IT, ale każdego, kto korzysta ze służbowego telefonu czy komputera i ma dostęp do firmowych danych. Jednym ze sposobów na wzrost świadomości wszystkich zatrudnionych są szkolenia w zakresie cyberbezpieczeństwa. Aby przyniosły one oczekiwany skutek, powinny być przeprowadzane regularnie, ze względu na wciąż zmieniające się techniki działań hakerów.

Źródło: Sprint S.A.

1. Źródło: „Cost of a Data Breach Report 2021”, IBM Security [↑](#footnote-ref-1)