HSBCnet

Business Email Compromise (BEC)

Ryzyko dla firmy:

Znaczna strata finansowa

Ryzyko utraty reputacji

W ostatnich latach systematycznie rośnie liczba ataków cybernetycznych. Przestępcy nieustannie opracowują nowe sposoby wykradania informacji i pieniędzy, a jednym z najnowszych zagrożeń jest tzw. Business Email Compromise.

Inne określenia tej metody to: oszustwo „na prezesa" • oszustwo „na dyrektora" • przekierowanie płatności • whaling

Jak działa Business Email Compromise

Oszust wysyła wiadomość email do firmowego zespołu ds. płatności, podając się za wykonawcę, dostawcę, wierzyciela lub nawet kogoś z kadry kierowniczej wyższego szczebla. Email sprawia wrażenie wiadomości od Dyrektora Generalnego, który prosi o dokonanie pilnej płatności, lub od dostawcy, który żąda, aby przyszłe płatności były kierowane na nowy rachunek. Często zawiera polecenie, aby nie omawiać tej kwestii z nikim innym.

Ponieważ adres poczty elektronicznej nadawcy jest specjalnie spreparowany tak aby był bardzo podobny do adresu znanego wcześnie odbiorcy, ten rodzaj oszustwa może pozostawać niezauważony do chwili, gdy jest już za późno... Cyberprzestępcy mogą nawet przejąć nielegalnie prawdziwe konto poczty elektronicznej, a wysyłane z niego fałszywe wiadomości mogą być trudne do zidentyfikowania.

Państwa informacje są cenne

Oszustwo może wydać się jeszcze bardziej przekonujące, jeżeli złodzieje pozyskają informacje o kierownictwie i zespole finansowym firmy, na przykład z jej strony internetowej.

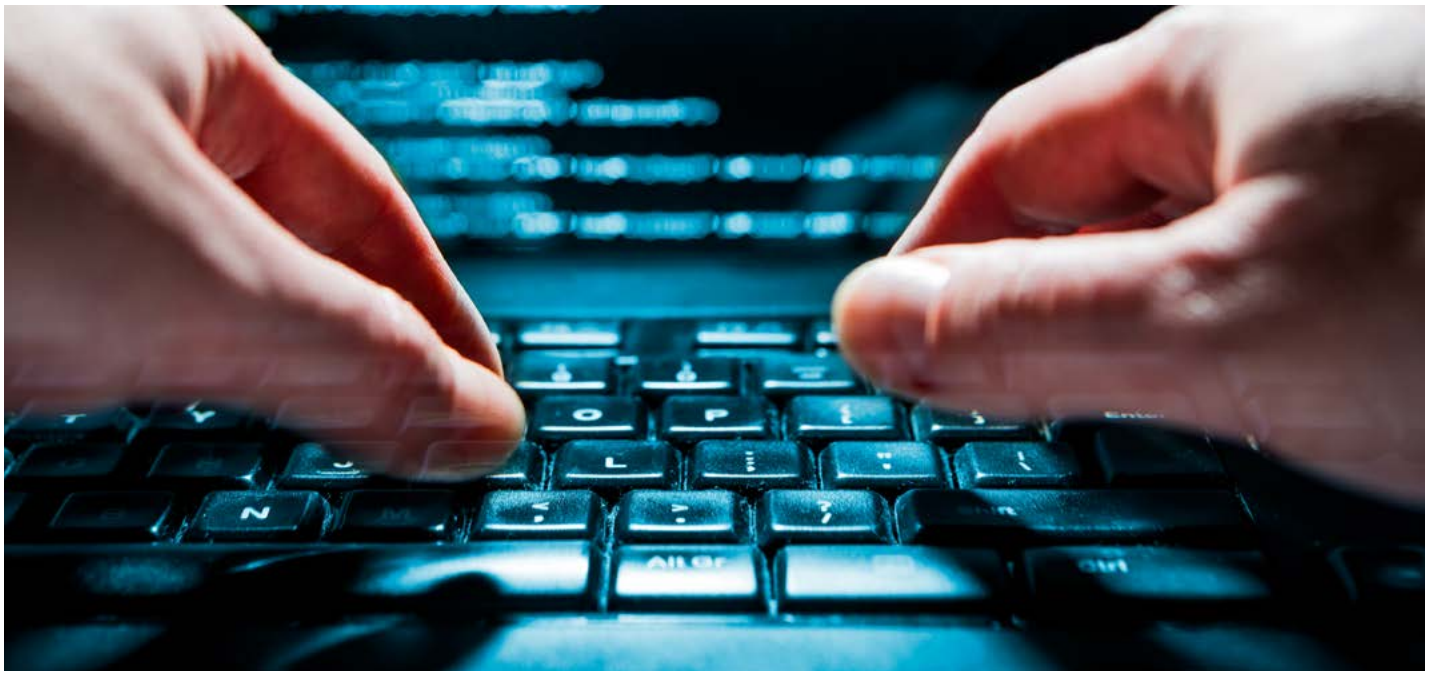
Z kolei posty w mediach społecznościowych mogą być źródłem informacji o tym, kiedy kadra kierownicza jest poza firmą, na spotkaniach lub na konferencjach. Dla oszusta jest to dobry moment na wysłanie wiadomości, ponieważ odbiorcy trudno jest zweryfikować autentyczność otrzymanej prośby czy polecenia.

Według FBI, w USA straty z tego tytułu są liczone w **setkach milionów dolarów.**
Średnia wyłudzona kwota to około

140 000 USD

Źródło: https://www.ic3.gov/media/2016/160614.aspx

HSBC



Business Email Compromise

opis prawdziwego przypadku: strata w wysokości 400 000 USD

Zespół ds. płatności otrzymał wiadomość email, która miała pochodzić od Dyrektora Generalnego firmy. Szef prosił o dokonanie płatności na rzecz nowych beneficjentów. Członek zespołu utworzył i zatwierdził płatności. Upłynęły dwa dni zanim zespół zdał sobie sprawę, że adres poczty elektronicznej osoby żądającej dokonania płatności nie był dokładnie taki sam jak adres Dyrektora Generalnego, a sprawca ukradł w tym czasie prawie 400 000 USD.

Od stycznia 2015 roku poziom odnotowywanych strat wzrósł o

1300%

a obecnie ich kwota wynosi ponad

3 miliardy USD

Źródło: https://www.ic3.gov/media/2016/160614.aspx

Jak zabezpieczyć swoją firmę:

- Należy upewnić się, że Państwa pracownicy są świadomi tego typu oszustwa.
- Należy wdrożyć wewnętrzny, dwustopniowy proces weryfikacji płatności, który obejmuje potwierdzenie żądania innymi metodami niż poczta elektroniczna.
- **Należy skontaktować się z osobą proszącą o dokonanie płatności pod zweryfikowanym numerem telefonu** w celu potwierdzenia żądania przesłanego pocztą elektroniczną.
  - NIE NALEŻY odpowiadać bezpośrednio na pierwszą wiadomość email.
  - NIE NALEŻY używać numerów telefonu ani innych informacji kontaktowych zawartych w wiadomości email.
- Należy sprawdzić, czy adresy poczty elektronicznej odpowiadają dokładnie adresom podanym w wewnętrznej dokumentacji firmy.
- Należy uważać na niespodziewane lub nieregularne żądania zapłaty, niezależnie od kwoty, której dotyczą. W razie wątpliwości nie należy dokonywać płatności.

W przypadku podejrzenia, że firma padła ofiarą oszustwa, należy skontaktować się bezpośrednio z przedstawicielem HSBC.