Czy moje dane zostały ujawnione?

Intensywnie analizujemy skutki incydentu. Pracujemy nad określeniem listy osób bezpośrednio dotkniętych jego skutkami. W przypadku stwierdzenia, że Pana/Pani dane zostały wykradzione z mFinanse, skontaktujemy się z Panem/Panią.

Co się dokładnie stało?

Przestępcy za pomocą złośliwego oprogramowania uzyskali czasowy dostęp do niektórych skrzynek pocztowych naszych pracowników. Część wiadomości zostało automatycznie przesłanych na serwery cyberprzestępców. Adresy e-mail zawarte w skradzionych wiadomościach służą im do dalszego rozsyłania złośliwego oprogramowania kolejnym osobom. Złośliwy kod zawarty jest w załączniku w formacie Microsoft Word o rozszerzeniu <.doc>. Otworzenie pliku powoduje zainfekowanie komputera.
Podjęliśmy działania zaradcze, sytuacja została opanowana.

Dostałem maila podszywającego się pod mFinanse. Otworzyłem załącznik, co mam zrobić?

W pełni skuteczne jest sformatowanie dysku systemowego i ponowna instalacja oprogramowania. Wcześniej należy wykonać skan wszystkich dysków aktualnym oprogramowaniem antywirusowym a następnie sporządzić kopię zapasową ważnych plików. Rekomendujemy zwrócenie się o pomoc do specjalisty informatyka.

Dostałem maila podszywającego się pod mFinanse. Nie otworzyłem załącznika, co mam zrobić?

Prosimy o skasowanie podejrzanej wiadomości. Prewencyjnie warto także zaktualizować system operacyjny i zeskanować komputer programem antywirusowym.

Co to jest podejrzany mail?

Zwróć uwagę, czy wyświetlana nazwa nadawcy jest tożsama z jego rzeczywistym adresem email. Przykładowy nagłówek fałszywej wiadomości:
Od: Imię Nazwisko <imie.nazwisko@mfinanse.pl> <rzeczywisty@adres.hacker.com>
To, co wydaje się być prawidłowym adresem email, czyli <imie.nazwisko@mfinanse.pl> jest tu tylko fragmentem nazwy użytkownika (wraz z imieniem i nazwiskiem stanowi tylko opis), a prawdziwy adres nadawcy, należący do przestępców, to rzeczywisty@adres.hacker.com. Każda zarażona wiadomość zawiera też załącznik Microsoft Word z rozszerzeniem <.doc > o przypadkowej nazwie oraz dodatkowe, dodane przez przestępców treści (takie jak powitanie) często - choć nie zawsze - w językach obcych.

mFinanse S.A. z siedzibą w Łodzi, ul. Kilińskiego 74, 90-119 Łódź, wpisana do rejestru przedsiębiorców KRS przez Sąd Rejonowy dla Łodzi-Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS pod nr KRS 0000365126, kapitał zakładowy (wpłacony w całości) 115.245.000 złotych, NIP 725 190 36 31

Nie chcę dostawać już od was tych wiadomości. Co mam zrobić? Co wy robicie, bym ich nie otrzymywał?

Te wiadomości nie pochodzą od nas. Wyglądają tak, jakby wysyłali je nasi pracownicy. Rzeczywiście wysyłają je cyberprzestępcy ze swoich serwerów. Nie mamy na to wpływu. Po otrzymaniu takiej wiadomości prosimy nie otwierać załącznika. Podejrzaną wiadomość proszę przesłać nam na adres zglos-incydent@mfinanse.pl. Następnie należy usunąć wiadomość.

Czy powinienem zmienić hasło do serwisu internetowego banku?

Zalecamy zmianę hasła, niezależnie od tego, jakie jest rzeczywiste ryzyko pozyskania przez przestępców dostępu do kont użytkowników systemów transakcyjnych banków. Czynności tej należy dokonać na zaufanym komputerze z aktualnym systemem operacyjnym i programem antywirusowym.
Dzięki wprowadzonym przez banki w tym miesiącu dodatkowym zabezpieczeniom dostępu do serwisów transakcyjnych przestępcy nie powinni mieć dostępu do Pani/ Pana konta użytkownika nawet, jeżeli hasło byłoby wykradzione.

Czy powinienem zmienić hasło do bankowości mobilnej (aplikacji na telefonie)?

Zalecamy zmianę hasła, niezależnie od tego, jakie jest rzeczywiste ryzyko pozyskania przez przestępców dostępu do kont użytkowników systemów transakcyjnych banków.