2018-06-21

UWAGA NA ZŁOŚLIWE OPROGRAMOWANIE W MAILACH

Ostrzegamy przed wciąż pojawiającymi się nowymi fałszywymi mailami z załącznikami rozsyłanymi za pośrednictwem poczty elektronicznej. Mail to wciąż powszechny środek komunikacji, dlatego jest najczęściej wykorzystywanym przez przestępców medium do infekowania komputerów użytkowników Internetu.

Cyberprzestępcy podszywają się pod różne firmy i kierują maile z zainfekowanym załącznikiem lub linkiem uruchamiającym instalację złośliwego oprogramowania. Załączniki przedstawiane są jako faktury, rachunki np. za energię czy telefon, informacje o przesyłce kurierskiej lub wygranej, czy potwierdzenie przelewu. Należy pamiętać, że pliki te niezależnie od rozszerzenia, również te popularne tj. *.doc, *.pdf, czy *.jpg, odpowiednio spreparowane przez przestępców mogą być również groźne. Czasem takie pliki dostarczane są w postaci zarchiwizowanej np. ZIP, RAR.

Celem tych działań jest najczęściej uzyskanie danych autoryzacyjnych do systemu bankowości elektronicznej lub przejęcia sesji komunikacyjnej z bankiem w celu podmiany numeru konta, na które wysyłamy pieniądze.

Jak się okazuje ten sposób wciąż jest skuteczny. Wiele osób daje się nabrać na tego typu informacje i otwiera zainfekowane załączniki lub linki, które uruchamiają instalację złośliwego oprogramowania na ich komputerze.

Dlatego przypominamy, że najlepszym sposobem, aby uchronić się przed tego typu atakiem, jest powstrzymanie się od otwierania załączników, klikania w linki w wiadomościach od nieznanych firm i osób. Nie należy otwierać załączników i klikać w linki również wówczas, gdy firma wydaje nam się znajoma, adres nadawcy wygląda poprawnie, ale nie spodziewamy się faktury, przelewu, czy wygranej z takiej firmy. W takich sytuacjach warto potwierdzić informację kontaktując się z taką firmą, należy jednak użyć adresu lub numeru telefonu znalezionego na stronie firmy lub publicznych katalogach, nie zaś w mailu z podejrzaną zawartością.

Przypominamy również o stosowaniu programów antywirusowych z włączoną automatyczną aktualizacją. Jest to podstawowe narzędzie chroniące komputer, dlatego powinno się znaleźć na każdym komputerze, a już koniecznie na tym, z którego logujemy się do bankowości elektronicznej.

Niezależnie od wspomnianych wyżej zabezpieczeń, namawiamy do każdorazowej weryfikacji informacji o przelewie z użyciem informacji podanych w SMS-owym potwierdzeniu przelewu (jeśli ta forma potwierdzeń jest używana) lub w potwierdzeniu przelewu (niestety, dopiero po jego zaksięgowaniu) w formie pliku pdf.

W sytuacji wątpliwości co do poprawności wysłanych przelewów, zwłaszcza w przypadku wcześniejszego otrzymania takiego maila i uruchomieniu załącznika lub linku, prosimy o pilny kontakt z Operatorami Tele-skok tel.: 801 800 100 lub (+48) 58 782 95 00