Wybrane problemy cyberbezpieczeństwa na przykładach scenariuszy ataków opartych na COVID-19

Agnieszka Gryszczyńska
Katedra Prawa Informatycznego, Wydział Prawa i Administracji, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie

Pandemia COVID -19 znacząco wpłynęła na metody pracy, nauki czy realizacji zadań publicznych. Nagłe zmiany i szerokie wykorzystanie zdalnej pracy czy nauki sprawiły, że uwidoczniły się problemy związane z cyberbezpieczeńswem. Pandemia COVID – 19 dla cyberprzestępców stała się okazją do zwiększenia skuteczności ataków opartych na socjotechnice. Niezwykle szybko przestępcy dostosowali dotychczasowe scenariusze ataków, zwłaszcza te prowadzące do przejęcia danych do logowania do bankowości elektronicznej czy portali społecznościowych. Już w dniu 13.3.2020 r. dystrybuowane były wiadomości SMS, w których nakłaniano do opłacenia szczepienia czy zalogowania się do bankowości elektronicznej w celu zatrzymania środków, które rzekomo miały zostać przekazane do rezerwy NBP (dpdoplata[.]org). Sprawcy podszywali się również pod Ministerstwo Zdrowia (https://mzgov[.]net), oferując paczkę żywnościową. Zmieniły się również scenariusze ataków, w których sprawcy tworzą strony internetowe podszywające się pod portal informacyjny, w celu uzyskania danych do logowania do portali społecznościowych, a następnie wykorzystania przejętych kont przy przejmowaniu kont innych osób oraz dokonywania oszustw (fakt24warszawka[.]com[.]pl/, hxxps://warszawa-info24[.]pl, ikoronawirusnews[.]pl).

Sprawcy wskazanych powyżej oraz podobnych ataków pozostają najczęściej nieuchwytni z uwagi na stosowanie przez nich różnych metod ukrycia własnej tożsamości -w szczególności posługują się fikcyjną lub przejętą tożsamością przy rejestracji domen, kart SIM, korzystaniu z usług świadczonych drogą elektroniczną czy zakładaniu kont na giełdach kryptowalut.

Nowe zagrożenia skłaniają do dyskusji nad anonimowością przy korzystaniu z usług elektronicznych oraz metodami weryfikacji tożsamości osób, które z usług tych chcą korzystać. Zagadnienie te nierozerwalnie wiąże się z narastającym zjawiskiem kradzieży tożsamości. Kolejnym problem zarówno prawnym jak i technicznym jest blokowanie domen internetowych, które służą do wyłudzeń danych i środków finansowych. Z jednej strony niezbędna jest szybka detekcja nazw domenowych o określonej strukturze czy rejestrowanych na fikcyjne lub przejęte dane poprzez analizę danych pochodzących z rejestrów, od rejestratorów czy analizy certstream. Problem ten jest również problemem prawnym dotykającym gwarancji prawnych wolności informacyjnej, autonomii informacyjnej czy swobody prowadzenia działalności gospodarczej.

Podczas prezentacji wskazane zostaną wybrane postulaty zmian prawnych i organizacyjnych, które mogłyby zredukować ilość i skutki najczęstszych obserwowanych cyberataków bazujących na COVID-19.