Bogumił Szmańda
radca prawny

Phishing kontrolowany jako element treningu bezpiecznego zachowania w sieci a polskie prawo.

Phishing jest jednym ze sposobów ataku internetowego, polegającym na podszyciu się pod jakiś podmiot, w celu uzyskania informacji od ofiary tego czynu.
Zazwyczaj polega to na wysłaniu mejla łudząco podobnego do oryginalnego, wysyłanego np. z banku, serwisu społecznościowego, sklepu internetowego, firmy kurierskiej, itp.
W przesyłce takiej zwykle jest albo prośba o podanie danych osobowych, danych identyfikacyjnych w serwisie internetowym, albo odnośnik do strony udającej serwis danego podmiotu, na której to stronie wprowadza się dane identyfikacyjne, które następnie są przesyłane do sprawcy ataku.
Wyżej wymienione zachowanie przestępne jest penalizowane przez art. 190a § 2 Kodeksu karnego z dnia 6 czerwca 1997 r. (t.j. Dz. U. z 2017 r. poz 2204) - dalej KK.

Phishing kontrolowany symuluje wspomniane działania i jest elementem testów (treningów) bezpiecznego zachowania w sieci. Stosowane bywają one np. w wewnętrznej sieci przedsiębiorcy, w celu edukacji jego pracowników, uświadomienia zagrożeń internetowych i wyczulenia na nie, a także dla przetestowania ich zdolności prawidłowego reagowania na niebezpieczeństwa płynące z Internetu. Celem tego podszywania się nie jest więc uzyskania informacji, ale ma ono wymiar dydaktyczny i kontrolny.
Nie ma też niebezpieczeństwa, że osoba niepowołana – spoza grupy docelowej, dla której trening jest przygotowany - będzie miała do niego dostęp. Dane wprowadzane przez użytkownika (pracownika) nie są wysyłane poza lokalną sieć ani trwale zapamiętywane.
Phishing kontrolowany nie będzie więc przestępstwem, ponieważ nie wypełnia znamion czynu zabronionego (brak chęci wyrządzenia szkody), podobnie jak test penetracyjny nie wypełnia znamion czyny zabronionego z art. 267 § 1 i 2 KK.

Czy wykonujący symulację phishingu może narazić się na zarzuty cywilnoprawne ze strony podmiotu, pod który się podszywa?

Nie ulega wątpliwości, że serwis internetowy, albo jego część graficzna, ewentualnie konkretna strona internetowa, jest często przedmiotem prawa autorskiego, czyli utworem, jego częścią, ewentualnie drobnym utworem. Podobnie może być z wiadomością przesyłaną pocztą elektroniczną. Zgodnie z art. 29 Ustawy o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 r. (t.j. Dz. U. z 2017 r. poz. 880 z późn. zm.) – dalej PA, wolno przytaczać utwory lub ich urywki w innym utworze, jeżeli jest to uzasadnione celami cytatu. Niewątpliwie utworem, w rozumieniu tej ustawy, jest też system informatyczny do prowadzenia treningu bezpiecznego zachowania w sieci (Internecie), który zawiera w sobie symulację phishingu. Test taki wykorzystuje zazwyczaj jedynie szatę graficzną jednej ze stron WWW serwisu, która stanowi niewielki procent systemu testującego. Celem tego jest dokładne zapoznanie się z technikami hackerów, aby zrozumieć jak oni działają i gdzie może czyhać niebezpieczeństwo na użytkownika sieci. Cytowanie grafiki w całości jest uzasadnione, bo to jest

element, z którym bezpośrednio styka się odwiedzający stronę WWW. Celem tego dozwolonego zapożyczenia jest nauczanie korzystających z Internetu - jak prawidłowo zachować się w sieci i wyjaśnienie jak działają przestępcy komputerowi. Istnieje więc związek między wykorzystaną treścią a głównym dziełem – wspomnianym systemem informatycznym, bez czego cel przedsięwzięcia treningowego nie mógłby być osiągnięty. Takie podejście jest najbardziej skuteczne, ponieważ użytkownik ma możliwość uświadomienia sobie zagrożeń, a także swoich słabości podczas rzeczywistego użytkowania sieci. To cytowanie grafiki wydaje się więc jak najbardziej uzasadnione ze względu na swoją skuteczność i wiarygodność.

Po wpisaniu danych identyfikacyjnych na symulowanej stronie i ich zatwierdzeniu, powinna się pojawić informacja, że szata graficzna strony WWW została wykorzystana w celach treningowych (edukacyjnych, sprawdzających), a prawa do tego utworu lub jego części ma określony podmiot. Zasadne jest też wskazanie źródła cytatu, czyli np. adresu oryginalnej strony WWW. Ten komunikat zapewni realizację przepisu art. 34 PA o podaniu twórcy i źródła utworu.

Gdy firma znajduje się w treści utworu, podmiot będący przedsiębiorcą mógłby zarzucić naruszenie prawa do niej, wynikającego z art. 43^{10} Ustawy Kodeks cywilny z dnia 23 kwietnia 1964 r. (t.j. Dz.U. z 2017 r. poz. 459 z późn. zm.) – dalej KC. Działanie to nie wydaje się być bezprawne, ponieważ wynika z przepisów o cytowaniu utworu, w którym może zawierać się firma.

Podobnie rzecz się ma z czynem nieuczciwej konkurencji, o którym mowa w art. 5 Ustawy o zwalczaniu nieuczciwej konkurencji z dnia 16 kwietnia 1993 r. (t.j. Dz. U z 2003 r. nr 153 poz. 1502 z późn. zm) – dalej ZNK. Symulacja phishingu nie narusza interesu podmiotu (np. właściciela strony WWW) będącego przedsiębiorcą. Nie dochodzi tu do takiego naruszenia, bowiem użytkownik poddany symulowanemu atakowi dowie się o tym działaniu, a więc nie wystąpią żadne przesłanki, które mogłoby uzasadniać nieuczciwe postępowanie w stosunku do tego podmiotu i stawiać go w złym świetle.

Phishing kontrolowany jest zgodny również z art. 13 ust. 2 ZNK. Wprawdzie naśladowanie cech funkcjonalnych strony WWW - jej szaty graficznej, mogłoby wprowadzić w błąd użytkownika, jednak system treningowy, po wpisaniu i zatwierdzeniu danych przez użytkownika, poinformuje go o teście. Podobnie rzecz ma się z innymi formami takiego ataku, np. przy bezpośrednim wykorzystaniu wiadomości e-mail. Wyklucza więc to niekorzystny skutek dla podmiotu i użytkownika. Wręcz działania takie przyniosą korzyść im obu. Z serwisu naśladowanego będą korzystali świadomi użytkownicy, którzy wiedzą jak chronić swoje dane.

Jeżeli w cytowanej szacie graficznej będzie znajdował się znak towarowy, to wydaje się, że symulacja phishingu nie naruszy również Ustawy Prawo własności przemysłowej z dnia 30 czerwca 2000 r. (t.j. Dz. U. z 2017 r. poz. 776) – dalej PWP. Użycie go jest konieczne do wskazania przeznaczenia serwisu treningowego, jako narzędzia do nauki i rozpoznawania zagrożeń, np. fałszywych stron WWW konkretnych podmiotów. Możliwość takiego działania wynika z art. 156 ust. 1 pkt. 3) PWP.