Europejska Sieć Zapobiegania Przestępczości

Seria narzędzi EUCPN

Nr 13

Zapobieganie oszustwom indywidualnym

Streszczenie

Trzynasty zestaw narzędzi w serii opublikowanej przez Sekretariat EUCPN koncentruje się na zapobieganiu *oszustwom indywidualnym*. Prezydencja bułgarska (pierwsza połowa 2018 r.) postanowiła skupić się na:

„[...] *problemach związanych z oszustwami, a w szczególności na oszustwach telefonicznych. Ten rodzaj przestępczości stał się w ostatnich latach dochodową działalnością przestępczą, która rozwija się zarówno na poziomie krajowym, jak i transgranicznym. Grupy przestępcze specjalizujące się w tej działalności rozwijają się dynamicznie i uderzają w szerszą grupę ofiar. Biorąc pod uwagę aktywne uczestnictwo ofiar w scenariuszach przestępczych, a także wiążący się tym traumatyczny wpływ na ich psychikę, należy podjąć poważne działania zapobiegawcze, uwzględniając specyfikę na szczeblu lokalnym, krajowym i transgranicznym".*

Oszustwa indywidualne to taki rodzaj oszustw, w których przestępcy biorą na celownik indywidualnych obywateli. Ofiary są nakłaniane do współpracy, a następnie zostają oszukane. Nasze obecne rozumienie tego rodzaju oszustw wiąże się głównie z jego współczesnymi formami, z których phishing służyłby prawdopodobnie za najlepszy przykład. Ważne jest jednak, aby uzmysłowić sobie, że indywidualne oszustwa istnieją od wieków. Ewolucja technologiczna z ostatnich dziesięcioleci pozwoliła na uprzemysłowienie tych oszustw na większą skalę niż kiedykolwiek uważano za możliwe. Kto choć raz w swoim życiu nie otrzymał e-maila z phishingiem?

Jak wyjaśniono w *uzasadnieniu* prezydencji bułgarskiej, ofiary aktywnie uczestniczą w swojej wiktymizacji. Sprawca skupia swoją uwagę na pieniądzach, ale może uzyskać do nich dostęp

tylko, jeśli przekona do tego swoją ofiarę. Zasadniczą taktyką przekonania ofiary do takiej uległości jest tzw. **inżynieria społeczna**. Pozwala ona sprawcy wzbudzić w ofierze pewność, która jest kluczowa dla sukcesu oszustwa. Psychologia społeczna pozwala nam lepiej zrozumieć to zjawisko. Odwołując się do codziennych zasad społecznych i wykorzystując tę „ludzką słabość", przestępcy są w stanie uruchomić coś, co nazywa się drugą ścieżką perswazji. Pierwsza ścieżka wymaga poważnego planowania i wysiłku poznawczego. Druga jednak nie wymaga konkretnego opracowania i otwiera furtkę do niemal nieświadomej reakcji. Przykładowo udając osobę sprawującą władzę, np. policjanta, sprawcy mogą z łatwością wymusić na swoich ofiarach odpowiedni poziom posłuszeństwa. Te społeczne i poznawcze reguły mają swoje codzienne zastosowania, jednak pozwalają przestępcom wykorzystywać je dla własnych korzyści.

Te zwodnicze taktyki są wykorzystywane w bardzo **wielu oszustwach**. *Szwindle nigeryjskie, przekręty na babcię lub prezesa, oszustwa z romansami*... możliwości jest tyle, na ile pozwala kreatywność oszustów. Ten bogaty wachlarz zwodniczych praktyk daje oszustom możliwość jednoczesnego wzięcia na celownik dużej grupy osób lub przyjęcie bardziej ukierunkowanego podejścia. Wydaje się, że w coraz większym stopniu popularyzuje się to drugie. Oszuści zdali sobie sprawę, że sprytne ukierunkowanie działań na ofiarę zapewni im większy „zwrot z inwestycji". E-maile typu phishing stają się coraz bardziej wyszukane i są adresowane do wyselekcjonowanych celów (grupy). Zaskakujący ostatni krok w tej ewolucji polega na połączeniu nowej i starszej technologii: telefonu. Vishing lub voice phishing (czyli „wyłudzenie głosowe") daje możliwość łączenia zalet zarówno internetu, jak i telefonu. Wykonanie telefonu online nie wiąże się prawie z żadnymi kosztami, jest trudniejsze do namierzenia i może być zautomatyzowane. Wykorzystanie telefonu niesie dodatkowe korzyści: ludzie bardziej ufają tej metodzie, a dzięki temu, że sytuacja staje się intymniejsza, ofiary są skuteczniej przekonywane. W celu zilustrowania rosnącego poziomu wyrafinowania dodajmy, że przestępcy zatrudniają nawet rodowitych użytkowników danego języka, aby rozmowy telefoniczne były jak najbardziej autentyczne.

Nasze obecne zrozumienie indywidualnych oszustw jest jednak ograniczone. Przestępstwa te wiążą się z ogromną **ciemną liczbą**, ponieważ wiele z nich pozostaje niezgłoszonych. Ofiary nie zdają sobie sprawy z tego, że padły ofiarą, nie postrzegają tej sytuacji jako wystarczająco poważnej, sądzą, że zgłoszenie niczego nie przyniesie lub po prostu nie wiedzą, gdzie powinny się zgłosić. Co więcej, ze względu na aktywną rolę, jaką ofiara odgrywa we własnej wiktymizacji, poczucie własnej winy i wstydu uniemożliwiają ofiarom opowiedzenie swojej

historii. Niektóre oszustwa uwzględniają nawet „wbudowane" mechanizmy zapobiegające zgłaszaniu, gdzie ofiary muszą podejmować nielegalne działania, obciążając w ten sposób samych siebie. Zgłaszając oszustwo, ofiara czułaby się tak, jak gdyby sama oddawała się w ręce policji.

Ciemna liczba przyczyniła się również do powstania **mitu**, że głównymi ofiarami tych przestępstw są osoby starsze, stanowiące łatwy cel. Niektóre badania obalają ten mit, choć należy zachować ostrożność ze względu na ograniczoną liczbę dostępnych publikacji. Niemniej jednak to młodsza populacja oraz osoby w średnim wieku zaliczają się do grup bardziej podatnych na oszustwa. Innym z krążących mitów jest to, że ofiarami stają się zazwyczaj osoby niewykształcone lub niedoświadczone finansowo, jednak w rzeczywistości wygląda to odwrotnie. Jednym z możliwych wyjaśnień jest tzw. „luka między wiedzą a działaniem", w której ludziom udaje się rozpoznać sygnały oszustwa, ale nie są oni w stanie zastosować tej wiedzy do własnej sytuacji.

Niestety mitem nie są tzw. „**listy frajerów**". Oszuści telefoniczni kontaktują się z ofiarami losowo lub korzystając z rejestrów publicznych, ale mogą także dzielić się między sobą listami celów, które zostały już oszukane. Stosowanie takich list wskazuje na wysoki poziom powtarzającej się wiktymizacji. Na przykład, niektórzy oszuści będą próbować „pomóc" ofiarom w odzyskaniu utraconych dóbr…

Ponieważ kontrola nad tymi oszustwami jest niezwykle trudna, potrzeba stosowania działań zapobiegawczych staje się wysoka. Jednakże przeprowadzono niewiele badań naukowych i analitycznych na temat oszustw indywidualnych. Niemniej jednak możemy przedstawić pewne ogólne ustalenia. Najpowszechniejszą taktyką zapobiegawczą jest edukacja społeczeństwa. Można to robić w ramach ogólnych kampanii podnoszenia świadomości, ale najlepiej, gdy jest to jakaś forma szkolenia, wówczas można zauważyć pewne pozytywne skutki. Zasadniczo szkolenia te starają się zlikwidować „lukę między wiedzą a działaniem", o której wspominaliśmy wcześniej. Inną kluczową taktyką jest praca z samymi ofiarami. Ze względu na ich aktywną rolę w procesie oraz istniejące ryzyko stania się ofiarą po raz kolejny, ofiary powinny otrzymać wsparcie oraz informacje o swojej specyficznej sytuacji.

Podczas prezydencji bułgarskiej Sekretariat zebrał szereg **dobrych praktyk** w tym zakresie. Można je podzielić według grup docelowych. Pierwsza kategoria skupia się na całej populacji. Są to kampanie uświadamiające, takie jak te z Bułgarii, Szwecji czy Belgii oraz te

przygotowane przez Europol. Obejmują one np. spoty radiowe, plakaty, ulotki czy gadżety, które dostarczają ludziom przydatnych informacji i pokazują, jak chronić się przed szkodliwymi działaniami. Drugi zestaw działań skierowany jest do osób starszych. W tym przypadku stosuje się bardziej interaktywne metody, jak ma to miejsce w Czechach. Osoby starsze biorą udział w interaktywnym przedstawieniu, w którym poznają najpowszechniejsze taktyki oszustów i uczą się, jak na nie reagować. To „żywe doświadczenie" powinno przełożyć się na odpowiednią reakcję w prawdziwym życiu. Ocena tego projektu wykazała, że jest to właściwe założenie, ponieważ grupa odmawiała fałszywym transakcjom dwa i pół raza częściej niż grupa kontrolna, która nie oglądała przedstawienia. Ostatnia kategoria działań prewencyjnych skupia się na ofiarach. Przykłady z Australii, Wielkiej Brytanii i Kanady wskazują na potrzebę prowadzenia tego rodzaju profilaktyki. Istnieje jednak – nawet w skali globalnej – niewiele usług wsparcia dla ofiar indywidualnych oszustw.

Sekretariat EUCPN zorganizował warsztaty z różnymi ekspertami w celu opracowania **zaleceń** dotyczących zapobiegania oszustwom telefonicznym. Są one zorganizowane zgodnie z pięcioma strategiami sytuacyjnego zapobiegania przestępczości. Pierwszą możliwą strategią jest zwiększenie wysiłków, jakie sprawca musi podjąć, aby oszustwo odniosło sukces. Skutecznym przykładem może tu być ograniczenie rozpowszechniania oraz dostępu do numerów telefonów. Inną techniką może być ograniczenie ilości numerów telefonów, które dana osoba może posiadać lub które można połączyć z kontem bankowym bądź numerem identyfikacyjnym.

Drugą strategią jest zwiększenie ryzyka. Kluczowe znaczenie ma tutaj dzielenie się informacjami. Taki proces udostępniania nie powinien kończyć się na granicach sektora publicznego czy prywatnego, ani na poziomie krajowym. Wszyscy partnerzy muszą odegrać ważną rolę w tej strukturze informacyjnej. Wiedza na temat tego, z czym ma się do czynienia, już na starcie zwiększa szanse uniknięcia oszustwa. Zrozumiałym jest, że sam proces zgłaszania powinien być łatwiejszy i przystępniejszy. Informacje muszą zostać zgromadzone, zanim będzie je można udostępnić. W innych zaleceniach postuluje się o zmniejszenie anonimowości rozmówcy, tak aby ujawnienie lokalizacji ofiary było praktycznie niemożliwe. Zastosowanie mogłoby tu także znaleźć oprogramowanie do rozpoznawania głosu.

Trzecią strategią zapobiegania oszustwom telefonicznym jest ograniczenie korzyści, które można osiągnąć poprzez popełnienie danego przestępstwa. Głównym zaleceniem jest tutaj zajmowanie nielegalnie pozyskanych zasobów. Aby było to możliwe, kluczowym jest

monitorowanie przepływu pieniędzy, które pozwoli wykrywać podejrzane transakcje. W celu ułatwienia realizacji tego zadania nasi eksperci rekomendują podjęcie inicjatywy dla całej UE z udziałem sektora bankowego.

Inną strategią jest ograniczenie prowokacji. W tym przypadku ważnym jest, aby nie udostępniać zbyt wiele informacji na temat tego, w jaki sposób oszustwo zostało faktycznie zrealizowane, gdyż pozwoli to zapobiec naśladownictwu. Poza tym może to pomóc w zapobieganiu niektórym formom powtarzającej się wiktymizacji. Ostatnią strategią jest pozbycie się wymówek. Działania te koncentrują się głównie na podnoszeniu świadomości o oszustwach telefonicznych oraz sposobach chronienia się przed nimi. Jako kluczowe przykłady przedstawiono tu dobre praktyki, które stosowano już wcześniej. Kampanie informacyjne powinny nieść to samo przesłanie. Dlatego też należy ustanowić jak najbardziej spójne partnerstwa między sektorem publicznym i prywatnym oraz współpracę międzynarodową: *wystarczy powiedzieć „nie”*.