Rekomendacja Rady ds. Cyfryzacji w zakresie ograniczenia kradzieży tożsamości oraz cyberataków wykorzystujących polską infrastrukturę z 14 kwietnia 2022r.

1. Podniesienie bezpieczeństwa domeny .pl

Z uwagi na to, że w części ataków obserwowanych w Polsce wykorzystywane są nazwy domenowe z domeny .pl lub domeny, gdzie rejestratorami (pośrednikami) są podmioty mające siedzibę na terytorium Polski, należy pilnie dokonać zmian w procesie pośrednictwa w rejestracji domen i nałożyć na rejestratorów obowiązki związane z weryfikacją tożsamości podmiotów rejestrujących nazwy domenowe (abonentów).

Aktualnie rejestratorzy opierają się na danych deklarowanych przez rejestrujących, co prowadzi do sytuacji, w której cyberprzestępcy na potrzeby rejestracji domeny podają dane innych podmiotów (zarówno osób fizycznych, jak i podmiotów prowadzących działalność gospodarczą) lub kreują nową tożsamość. Postuluje się w procesie weryfikacji danych abonenta wprowadzenie mechanizmów weryfikacji tożsamości z wykorzystaniem już istniejących narzędzi, takich jak wykorzystanie podpisów elektronicznych i pieczęci elektronicznych w rozumieniu e-IDAS (w tym w szczególności podpisu kwalifikowanego), podpisu osobistego (o którym mowa w ustawie o dowodach osobistych[1]), podpisu zaufanego (o którym mowa w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne[2]) lub innych mechanizmów, takich jak np. wideoweryfikacja.

Jawny rejestr domeny .pl powinien również zawierać dane kontaktowe do abonenta domeny (co najmniej adres e-mail). Aktualnie w bazie WHOIS nie są publikowane dane abonentów będących osobami fizycznymi. Dla porównania należy wskazać, że dla domeny *.eu baza WHOIS zawiera dane w postaci adresu mailowego abonenta.

Co więcej, należy również dokonywać lepszej weryfikacji podmiotów świadczących usługi pośrednictwa przy rejestracji nazw w domenie .pl (rejestratorów), w celu podniesienia poziomu cyberbezpieczeństwa i zapewnienia szybkiego reagowania pośredników na incydenty bezpieczeństwa związane z zarejestrowaną przez nich nazwą w domenie .pl.

W związku z nasilającymi się aktualnie atakami dezinformacyjnymi – należy poddać weryfikacji, jakie ciągi znaków wykluczyć z możliwości rejestracji jako nazwę domenową z rejestru .pl (dla przykładu w dniu 22.02.2022 roku osoba fizyczna dokonała rejestracji nazwy domenowej charlie-crp.pl, pośrednikiem w rejestracji był Aftermarket.pl Limited z siedzibą na Cyprze).

2. Lepsza weryfikacja tożsamości korzystających z elektronicznych usług publicznych.

[1] Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2022 r. poz. 671)
[2] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070)

Weryfikację tożsamości przy korzystaniu z dostępu do usług publicznych należy opierać na zaufanym profilu, certyfikacie kwalifikowanym i mechanizmach zawartych w warstwie elektronicznej dowodu osobistego, nie zaś na podawaniu numeru PESEL, który dostępny jest w wielu publicznie dostępnych rejestrach publicznych, zatem nie powinien być wykorzystywany jako dana weryfikująca tożsamość lub służąca do autoryzacji.

3. Blokowanie „złośliwych domen".

Za pozytywny krok w kierunku ochrony użytkowników Internetu przed wyłudzeniami uznać należy porozumienie z 23.03.2020 r. o utworzeniu listy ostrzeżeń odnoszącej się do domen internetowych, które służą do wyłudzeń danych i środków finansowych, którego sygnatariuszami są MC, NASK - PIB, Orange Polska S.A., Polkomtel Sp. z o.o., P4 Sp. z o.o. oraz T-Mobile Polska S.A. Z uwagi na to, że lista ostrzeżeń jest rozwiązaniem prowadzonym zgodnie z porozumieniem w okresach stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego należy kontynuować prowadzenie listy ostrzeżeń również po zakończeniu pandemii.

Co więcej konieczne jest wprowadzenie ustawowej podstawy prowadzenia listy ostrzeżeń (np. w uKSC) oraz obowiązków blokowania przez określone podmioty (np. wszystkich przedsiębiorców telekomunikacyjnych) nazw domenowych wpisanych na listę ostrzeżeń.

4. Podniesienie cyberbezpieczeństwa usług świadczonych drogą elektroniczną.

Dla podniesienia poziomu bezpieczeństwa i przeciwdziałania zjawisku kradzieży tożsamości celowe jest wprowadzenie obowiązków dotyczących lepszej weryfikacji tożsamości podmiotów korzystających z usług podmiotów świadczących usługi drogą elektroniczną. Aktualnie niemożliwe jest ustalenie danych osoby, która korzysta z konta poczty elektronicznej (np. podanego podczas rejestracji), a podmioty świadczące usługi drogą elektroniczną nie mają obowiązków związanych z gromadzeniem i przechowywaniem logów dostępowych użytkowników. W efekcie to regulamin danego podmiotu, a nie przepis prawa powszechnie obowiązującego decyduje o tym, czy i z jakiego okresu można uzyskać dane dotyczące adresów IP, z których logowano się do konta poczty elektronicznej (okres ten w Polsce, zgodnie z regulaminami różnych podmiotów, jest różny i wynosi od kilku do kilkunastu miesięcy). Powoduje to nie tylko brak możliwości ustalenia, kto korzysta z konta poczty elektronicznej, ale znacząco utrudnia lub wręcz uniemożliwia przeprowadzenie postępowania dotyczącego uzyskania nieuprawnionego dostępu (włamania) do takiego konta. Co więcej często w tworzeniu konta w celu przestępczym (widoczne jest to szczególnie w sprawach kierowania gróźb karalnych oraz kaskadowych alarmach bombowych) sprawcy wykorzystują dane osobowe innych osób w celu skierowania na nie podejrzeń. Na forach przestępczych polecane są w szczególności konta z domeny onet, z uwagi na to, że podczas rejestracji możliwe jest podanie numeru telefonu – jednak numer ten nie jest w żaden sposób weryfikowany. Pozwala to na podanie numeru telefonu osoby, pod którą sprawcy chcą się podszyć i na którą chcą skierować podejrzenia.

Istotnym problemem jest również zakres danych gromadzonych i udostępnianych jako „logi". Znaczna część podmiotów świadczących usługi drogą elektroniczną czy banków nie gromadzi bowiem informacji o portach. Z uwagi na to, że operatorzy bardzo szeroko wykorzystują NAT i jeden publiczny adres IP przydzielony może być nawet kilkudziesięciu tysiącom użytkowników, niemożliwe jest ustalenie abonenta usługi. Postuluje się zatem wprowadzenie weryfikacji tożsamości osób zakładających konta poczty elektronicznej, lepszą weryfikację tożsamości użytkowników elektronicznych usług świadczonych drogą elektroniczną oraz ustalenie jednolitego okresu przechowywania oraz struktury logów.

5. Zwiększenie wiarygodności danych abonentów usług telekomunikacyjnych.

W związku z rejestracją kart SIM na dane osób, których dane osobowe zostały nielegalnie pozyskane, rozważyć można nałożenie na operatorów telekomunikacyjnych obowiązków lepszej weryfikacji tożsamości osób, na których dane rejestrowane są karty przedpłacone lub na rzecz których świadczone są usługi telekomunikacyjne oraz obowiązków monitorowania anomalii (np. faktu rejestracji na jedną osobę fizyczną kilkuset lub kilku tysięcy kart przedpłaconych) i podejmowania bezzwłocznych działań mających na celu dezaktywację usług przedpłaconych w sytuacji ustalenia, że do aktywacji karty SIM posłużono się danymi osobowymi innej osoby. Celowe jest wprowadzenie w sytuacji nabycia karty przedpłaconej od innego podmiotu obowiązku ponownej rejestracji takiej karty pod rygorem dezaktywacji usługi.

Konieczne jest też zapewnienie lepszej weryfikacji tożsamości osób składających wniosek o wydanie duplikatu karty sim (przeciwdziałanie atakom SIM – SWAP). Jedną z barier do efektywnej współpracy pomiędzy bankami i przedsiębiorcami telekomunikacyjnymi jest brak możliwości wymieniania się informacjami objętymi tajemnicą bankową lub tajemnicą telekomunikacyjną. Do ograniczenia ataków SIM SWAP, włamań do rachunków bankowych oraz prania pieniędzy pochodzących z przestępstw może przyczynić się wprowadzenie przepisów ułatwiających wymianę informacji o ustalonych zdarzeniach pomiędzy operatorami telekomunikacyjnymi i bankami (np. o wydaniu karty SIM, wykorzystaniu danego numeru MSISDN do wysyłki SMS ze złośliwymi linkami, ustaleniu numeru MSISDN przypisanego do rachunku służącego do prania pieniędzy itp.).

Dla umożliwienia prowadzenia ustaleń dotyczących tożsamości osoby, która logowała się do rachunku, banki powinny mieć obowiązek gromadzenia i przekazywania na żądanie organów ścigania również informacji o numerze portu.

Operator telekomunikacyjny powinien ponosić odpowiedzialność cywilną (odszkodowawczą) oraz administracyjną (kary finansowe) za wydanie duplikatu karty SIM osobie nieuprawnionej oraz za niedokonanie dezaktywacji numerów MSISDN zarejestrowanych na dane ofiar kradzieży tożsamości lub zaistnienie anomalii polegającej na rejestracji wielu numerów MSISDN na dane jednej osoby fizycznej.

6. Przeciwdziałanie SMShingowi, VIShingowi i Spoofingowi.

Celowe jest nałożenie na przedsiębiorców telekomunikacyjnych obowiązków związanych z zapobieganiem nadużyciom związanych z dystrybucją phishingowych wiadomości SMS (zawierających odnośniki prowadzące do stron internetowych wyłudzających dane do logowania lub środki finansowe) poprzez blokowanie SMS zawierających nazwy domenowe wpisane na listę ostrzeżeń CSIRT NASK.

Konieczne jest również ograniczanie nadużyć telekomunikacyjnych, w tym simboxingu oraz spoofingu. Docelowo, choć wymaga to odpowiedniego przygotowania, postulować można zastąpienie protokołów komunikacyjnych SS7 (Signaling System 7), protokołem STIR/SHAKEN. Wdrożenie STIR/SHAKEN wymaga jednak czasu oraz zapewnienia środków finansowych. Co więcej, aby wdrożenie STIR/SHAKEN skutecznie ograniczało zjawisko IDCaller spoofing konieczne jest, aby protokół ten stał się międzynarodowym standardem i został wdrożony przez wszystkich operatorów.

Zapewnienie bezpieczeństwa i integralności usług oraz przekazu telekomunikacyjnego jest obowiązkiem operatorów telekomunikacyjnych, który powinien być realizowany i egzekwowany. Problem spoofingu znany jest od wielu lat i mimo upływu czasu bardzo niewiele zrobiono, by temu zjawisku przeciwdziałać, tak w skali pojedynczych operatorów, jak ich partnerów zagranicznych (umowy interconnectowe) i regulacji międzynarodowej. Potrzebne jest podjęcie inicjatyw w tym zakresie w UE i w światowych organizacjach telekomunikacyjnych. Warto skorzystać z doświadczeń np. USA i Kanady, które podjęły skuteczną walkę ze spoofingiem przy zaangażowaniu zarówno administracji, jak i samych operatorów telekomunikacyjnych.

7. **Poprawa bezpieczeństwa dystrybucji i synchronizacji czasu dla przemysłu opartego na systemie operacyjnym LINUX i używającego serwerów LINUX.**

Wskazujemy na celowość poprawienia i wzmocnienia cyberbezpieczeństwa krajowego przemysłu IT/OT opartego na systemie operacyjnym LINUX i używającego serwerów LINUX do synchronizacji czasu, w tym szczególności rekomendujemy uruchomienie i wsparcie projektów mających na celu instalację w serwerowniach podmiotów publicznych i prywatnych grupy specjalnie przygotowanych serwerów NTP i zadeklarowania ich do puli PL.NTPPOOL.ORG.

8. **Przyśpieszenie działań zmierzających do powołania sektorowych zespołów cyberbezpieczeństwa (CSIRT).**

W ustawie o krajowym systemie cyberbezpieczeństwa wprowadzona została możliwość powoływania sektorowych zespołów cyberbezpieczeństwa, określanych również jako CSIRT-y sektorowe. Od czasu wprowadzenie w życie ustawy w 2018, powstał tylko jeden taki zespół. Powołała go Komisja Nadzoru Finansowego - organ właściwy dla sektora finansowego. Tym zespołem jest CSIRT KNF.

Praktyka, w tym sposób zarządzania i koordynacji działań w trakcie obowiązywania stopni alarmowych CRP, wskazuje na to, że działania ośrodka realizującego funkcje CSIRT-u sektorowego, pozytywnie wpływają na sytuację w sektorze. Również działania w okresach

nie objętych takimi stopniami bardzo pozytywnie wpływają na systematyczne podnoszenie poziomu cyberbezpieczeństwa. Dodatkowo projekt nowelizacji UoKSC przewiduje obowiązkowe powołanie takich zespołów, co jest jednoznacznym sygnałem co do przekonania o skuteczności tego rozwiązania.

Proponujemy, aby podjąć pilne działania, aby już teraz w oparciu o obowiązujące przepisy, przyśpieszyć działania zmierzające do powołania sektorowych zespołów CSIRT przez poszczególne organy właściwe. W sytuacji szczególnego zagrożenia, z jakim mamy obecnie do czynienia, powinno to odegrać bardzo istotną rolę w podwyższeniu zdolności do obrony w cyberprzestrzeni, w poszczególnych sektorach usług kluczowych.

9. Tworzenie Centrum wymiany i analiz ISAC.

Centrum wymiany informacji i analiz (ISAC) to w założeniu zaufana jednostka sektorowa lub międzysektorowa (obejmująca różne środowiska, służby i ekspertów ze sfery publicznej, jak i prywatnej), która może zapewnić 24/7 bezpieczną zdolność operacyjną, realizująca wymagania dotyczące koordynacji, udostępniania informacji i analizy w przypadku incydentów cybernetycznych, zagrożeń i luk w zabezpieczeniach sieci teleinformatycznych. Z jednej strony ISAC może służyć jako zasób branżowy, dzięki któremu można gromadzić kluczowe informacje o zdarzeniach i problemach związanych z cyberbezpieczeństwem w danej branży oraz identyfikować, komunikować się i analizować potencjalne skutki takich problemów dla danego sektora. Z drugiej strony powstanie ISAC niekoniecznie musi wiązać się z realizacją działań jedynie w określonej branży, co zwiększa zdolności w obszarze jedynie danego sektora. Koordynacja może dotyczyć wspólnych przedsięwzięć, czy wspólnych celów związanych potrzebą zapewnienia ochrony systemowej. Wspólnym mianownikiem dla działań partnerów w obszarze cyberbezpieczeństwa jest często charakter strategiczny ich usług, stanowiących ważny element na mapie infrastruktury krytycznej Państwa. Obecnie istnieje znacząca potrzeba dalszego rozszerzenia roli ISAC. Ta potrzeba jest również przedstawiona w ostatniej nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa.

Jest oczywiste, że ten rodzaj współpracy wspiera budowanie zaufania i wymianę informacji o incydentach / zagrożeniach między podmiotami i wyraźne określa cyberbezpieczeństwo jako priorytet na szczeblu krajowym i na poziomie międzynarodowym. Jednocześnie wiele ISAC wciąż poszukuje wzorców i dodatkowych obowiązków, aby się rozwijać i ewoluować, aby móc przede wszystkim oprzeć się bardziej zaawansowanym atakom.

10. Przyspieszenie prac nad nowelizacją ustawy o KSC

Przewidywana w projekcie nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa, instytucja dostawców wysokiego ryzyka nabiera w świetle agresji Rosji na Ukrainę także nowego wymiaru – ochrony, przed zagrożeniami ze strony dostawców powiązanych z Rosją, podmiotów operujących na polskim rynku, a także sankcji Polski względem Rosji. W obecnej sytuacji geopolitycznej dla zwiększenia poziomu bezpieczeństwa celowe jest przyspieszenie prac nad nowelizacją uKSC.