Problemy analizy danych wynikające z ochrony informacji prawnie chronionych w sektorze bankowym

FinCERT.pl

Warszawa, 6 czerwca 2019 r.

ZWIĄZEK BANKÓW POLSKICH

FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP

- FinCERT pl Bankowe Centrum Cyberbezpieczeństwa ZBP jednostka operacyjna funkcjonująca w Zespole Bezpieczeństwa Banków ZBP
- Współpracujemy z podmiotami wspomagającymi obszar bankowy na terenie Polski oraz z podmiotami zagranicznymi
- Koordynuje obsługę incydentów zagrażających cyberbezpieczeństwu banków oraz ich klientów
- 31.07.2017 r. – Bankowe Centrum Cyberbezpieczeństwa jako CERT – akredytacja Carnegie Mellon University;
- 01.01.2019 r. – 32 banki (29 – SA, 1 – BP, 2 – BS) – 95,23% udziałów w sumie aktywów wszystkich banków oraz 97,05% udziałów w sumie aktywów banków w formie SA i BP

ZWIĄZEK BANKÓW POLSKICH

Niektóre zdarzenia obsługiwane przez FinCERT.pl

- Obsługujemy zdarzenia transgraniczne typu BEC -Business Email Compromise;
- Koordynujemy działania sektora bankowego z innymi, Policją oraz pozostałymi podmiotami mającymi wpływ na cyberbezpieczeństwo;
- Koordynujemy sprawy na terenie Polski, a jeśli jest to konieczne także za granicami kraju;
- Identyfikujemy i blokujemy strony Phishingowe oraz informujemy o nich banki;
- Analizujemy pojawiające się informacje o aplikacjach mobilnych zawierających niepożądaną funkcjonalność;
- Identyfikujemy i blokujemy oszukańcze sklepy internetowe;
- Koordynujemy działania które ze względu na skalę wymagają współdziałania wielu podmiotów (np. sim-swap);
- Współuczestniczymy w działalności edukacyjnej o cyberbepieczeństwie skierowanej do klientów banków oraz pracowników instytucji finansowych;
- Koordynujemy incydenty o skutkach międzysektorowych.

ZWIĄZEK BANKÓW POLSKICH

Przetwarzanie i udostępnianie informacji objętych tajemnicą bankową w ramach sektora bankowego

- Art. 106d ust. 1 Prawa bankowego

Banki, inne instytucje ustawowo upoważnione do udzielania kredytów, instytucje utworzone na mocy art. 105 ust. 4, instytucje pożyczkowe, podmioty, których podstawowa działalność polega na udostępnianiu składników majątkowych na podstawie umowy leasingu, oraz podmioty, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą bankową, w przypadkach:

1) uzasadnionych podejrzeń, o których mowa w art. 106a ust. 3;

2) uzasadnionych podejrzeń popełnienia przestępstw dokonywanych na szkodę banków, innych instytucji ustawowo upoważnionych do udzielania kredytów, instytucji kredytowych, instytucji finansowych, instytucji pożyczkowych oraz podmiotów, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, i ich klientów, w celu i zakresie niezbędnym do zapobiegania tym przestępstwom.

ZWIĄZEK BANKÓW POLSKICH

Przetwarzanie i udostępnianie informacji objętych tajemnicą bankową w ramach sektora bankowego

- Art. 106d ust. 2 Prawa bankowego

Podmioty określone w ust. 1 mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą bankową oraz informacje dotyczące wyroków skazujących, w przypadkach przestępstw dokonywanych na szkodę banków, innych instytucji ustawowo upoważnionych do udzielania kredytów, instytucji kredytowych, instytucji finansowych, instytucji pożyczkowych oraz podmiotów, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, i ich klientów, w celu i zakresie niezbędnym do zapobiegania tym przestępstwom.

ZWIĄZEK BANKÓW POLSKICH

Przetwarzanie i udostępnianie informacji objętych tajemnicą bankową w ramach sektora bankowego

- Art. 106 ust. 1 Prawa bankowego

Bank jest obowiązany przeciwdziałać wykorzystywaniu swojej działalności dla celów mających związek z przestępstwem, o którym mowa w art. 165a lub art. 299 Kodeksu karnego

- Art. 106a ust. 1 Prawa bankowego

W razie zaistnienia uzasadnionego podejrzenia, że działalność banku jest wykorzystywana w celu ukrycia działań przestępczych lub dla celów mających związek z przestępstwem skarbowym lub innym przestępstwem niż przestępstwo, o którym mowa w art. 165a lub art. 299 Kodeksu karnego - bank zawiadamia o tym prokuratora, Policję albo inny właściwy organ uprawniony do prowadzenia postępowania przygotowawczego.

ZWIĄZEK BANKÓW POLSKICH

Przetwarzanie i udostępnianie informacji objętych tajemnicami pomiędzy sektorem bankowym a sektorem telekomunikacyjnym

- Art. 159 Prawa telekomunikacyjnego – tajemnica telekomunikacyjna

1. Tajemnica komunikowania się w sieciach telekomunikacyjnych, zwana dalej "tajemnicą telekomunikacyjną", obejmuje:

1) dane dotyczące użytkownika, z zastrzeżeniem art. 161 ust. 2;

2) treść indywidualnych komunikatów;

3) dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne, w tym dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej lub w ramach usług telekomunikacyjnych wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych;

4) dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku;

5) dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń.

ZWIĄZEK BANKÓW POLSKICH

Przetwarzanie i udostępnianie informacji objętych tajemnicami pomiędzy sektorem bankowym a sektorem telekomunikacyjnym

- Art. 159 Prawa telekomunikacyjnego – tajemnica telekomunikacyjna

2. Zakazane jest zapoznawanie się, utrwalanie, przechowywanie, przekazywanie lub inne wykorzystywanie treści lub danych objętych tajemnicą telekomunikacyjną przez osoby inne niż nadawca i odbiorca komunikatu, chyba że:

1) będzie to przedmiotem usługi lub będzie to niezbędne do jej wykonania;

2) nastąpi za zgodą nadawcy lub odbiorcy, których dane te dotyczą;

3) dokonanie tych czynności jest niezbędne w celu rejestrowania komunikatów i związanych z nimi danych transmisyjnych, stosowanego w zgodnej z prawem praktyce handlowej dla celów zapewnienia dowodów transakcji handlowej lub celów łączności w działalności handlowej;

4) będzie to konieczne z innych powodów przewidzianych ustawą lub przepisami odrębnymi.

3. Z wyjątkiem przypadków określonych ustawą, ujawnianie lub przetwarzanie treści albo danych objętych tajemnicą telekomunikacyjną narusza obowiązek zachowania tajemnicy telekomunikacyjnej.

4. Przepisów ust. 2 i 3 nie stosuje się do komunikatów i danych ze swojej istoty jawnych, z przeznaczenia publicznych lub ujawnionych postanowieniem sądu wydanym w postępowaniu karnym, postanowieniem prokuratora lub na podstawie odrębnych przepisów.

ZWIĄZEK BANKÓW POLSKICH

Przetwarzanie i udostępnianie informacji objętych tajemnicami pomiędzy sektorem bankowym a sektorem telekomunikacyjnym

- Przykład 1

„Witam Was,

Trochę idąc za ciosem a trochę w sposób niekontrolowany wyszła nam pilna sprawa z klientem jednego z banków. Otóż zainstalował sobie aplikację Crypto.Monitor. Niestety jak łatwo się domyślić robiła także rzeczy co do których klient nie miał świadomości. Generalnie został trafiony.

Mamy obecnie w BCC w analizie tą apkę. Niestety jej kod na niewiele daje nam informacji z czym się łączy i z jakich adresów jest administrowana (tj. skąd jakie komendy, gdzie śle jakie komunikaty). Wiemy natomiast, że jest ona w obrocie pośród klientów wielu banków Członków BCC.

Czy i w jakim zakresie jesteście w stanie nam pomóc w analizie ruchu jaki był prowadzony z numerem XXXXXXXX ? Dodatkowo zawężamy poszukiwania do daty XXXXXX.Klient co prawda twierdzi, że instalował aplikację około miesiąc przed tą datą ale XXXXX doszło do kilku niepokojących zdarzeń zakończonych w tym dniu około XXXX totalnym resetem urządzenia mobilnego.

Czy możecie nam pomóc w ustaleniu z jakimi adresami serwerów łączył się ten numer, jak przebiegała komunikacja pakietowa do i z tego numeru?”

ZWIĄZEK BANKÓW POLSKICH

Przetwarzanie i udostępnianie informacji objętych tajemnicami pomiędzy sektorem bankowym a sektorem telekomunikacyjnym

- Przykład 1

„Dobry wieczór,

W odpowiedzi do maila poniżej oraz w nawiązaniu do ostatniego spotkania (…) informuję, że wnioskowane dane są objęte tajemnicą telekomunikacyjną, o której mowa w art. 159 ust. 1 Prawa telekomunikacyjnego, a XXX jako podmiot uczestniczący w wykonywaniu działalności telekomunikacyjnej (…) jest obowiązana do zachowania tej tajemnicy.

Informacje objęte tajemnicą telekomunikacyjną mogą być wydane/udostępnione po otrzymaniu postanowienia Prokuratora w sprawie zwolnienia XXX z tajemnicy telekomunikacyjnej wydanego w trybie art. 218 § 1 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego.

Zatem najlepszym rozwiązaniem będzie zgłoszenie się osoby poszkodowanej na Policję lub do prokuratury w celu złożenia zawiadomienia o możliwości popełnienia przestępstwa”.

ZWIĄZEK BANKÓW POLSKICH

Przetwarzanie i udostępnianie informacji objętych tajemnicami pomiędzy sektorem bankowym a sektorem telekomunikacyjnym

Przykład 2 - oszukańcze platformy internetowe umożliwiających rzekome dokonywanie transakcji FOREX

Prokuratura przekazała ZBP m.in.:

- nr rachunków bankowych przestępców, na które pokrzywdzeni przelewają środki;
- treść powtarzalnego komunikatu, jaki pojawia się w polu opis transakcji w transakcji przelewów identyfikującego przelewy osób oszukiwanych (próba identyfikacji nieznanych jeszcze rachunków biorących udział w procederze);
- numery IP, jakie pojawiają się w kontekście działalności przestępczej (posłużą do identyfikacji prawdopodobnej komunikacji sprawców z Bankami oraz prawdopodobnych nowych kontekstów tej komunikacji).

ZWIĄZEK BANKÓW POLSKICH

Przetwarzanie i udostępnianie informacji objętych tajemnicami pomiędzy sektorem bankowym a sektorem telekomunikacyjnym

Przykład 2 - oszukańcze platformy internetowe umożliwiających rzekome dokonywanie transakcji FOREX

- Jak udało się zidentyfikować inne rachunki wykorzystywane przez przestępców?

1. Banki przekazały operatorom informacje o numerach telefonów przypisanych do rachunków.
2. Prokuratura zwolniła operatorów z tajemnicy telekomunikacyjnej.
3. Operatorzy przekazali Prokuraturze informacje o innych numerach telefonów powiązanych z przekazanymi numerami.
4. Prokuratura przekazała zidentyfikowane numery bankom.
5. Na tej podstawie banki zidentyfikowały rachunki wykorzystywane przez przestępców.

ZWIĄZEK BANKÓW POLSKICH

Przetwarzanie i udostępnianie informacji objętych tajemnicami pomiędzy sektorem bankowym a sektorem ubezpieczeniowym

- Art. 35 ustawy o działalności ubezpieczeniowej i reasekuracyjnej

1. Zakład ubezpieczeń i osoby w nim zatrudnione, a także osoby i podmioty, za pomocą których zakład ubezpieczeń wykonuje czynności ubezpieczeniowe, są obowiązane do zachowania tajemnicy dotyczącej poszczególnych umów ubezpieczenia.

2. Obowiązek zachowania tajemnicy, o którym mowa w ust. 1, nie dotyczy informacji udzielanych na wniosek: (….) */m.in. Sąd, prokuratura, Policja, ABW o ile są niezbędne w postępowaniu/*

(…)

5. Zakład ubezpieczeń może udostępniać dane dotyczące umów ubezpieczenia na zasadach i w trybie określonych w ustawie z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych (Dz. U. z 2018 r. poz. 470, z późn. zm.).

6. Nie narusza obowiązku zachowania tajemnicy, o którym mowa w ust. 1, złożenie zawiadomienia o podejrzeniu popełnienia przestępstwa na szkodę zakładu ubezpieczeń albo o tym, że działalność zakładu ubezpieczeń jest wykorzystywana w celu ukrycia przestępstwa lub przestępstwa skarbowego lub dla celów mających związek z przestępstwem lub przestępstwem skarbowym.

(…)

ZWIĄZEK BANKÓW POLSKICH

Przetwarzanie i udostępnianie informacji objętych tajemnicami pomiędzy sektorem bankowym a sektorem ubezpieczeniowym

- Przykład 1

Do zakładu ubezpieczeń zgłoszono roszczenia powstałe w wyniku zagubienia bagażu. Zgodnie z umową przysługiwało odszkodowanie w wysokości 100% sumy ubezpieczenia. Należało przedstawić spis rzeczy, które znajdowały się w walizce. Tymi rzeczami były dobra luksusowe kupowane m.in. w takich sieciach, jak Louis Vuitton, Boss, Prada itd.

Po wpłynięciu roszczeń w pierwszej kolejności ubezpieczyciel zweryfikował dokumentację przedkładaną przez klientów. Efekty ustaleń:

1. Dokumentacja z linii lotniczych potwierdzająca zagubienia bagażu okazała się sfałszowana.
2. W przypadku zagubienia bagażu najprawdopodobniej druga osoba współpracująca z roszczącym zabierała daną walizkę z taśmy po przylocie.
3. Zakład odkrył również proceder polegający na tym, że dobra były faktycznie kupowane, a poza zwracaniem się o odszkodowanie, osoby zgłaszały reklamacje w swoim banku związaną z nieuprawnionym użyciem karty.

- *Analiza danych dotyczących przestępstw ujawnionych w 2014 r. w związku z działalnością zakładów ubezpieczeń – członków Polskiej Izby Ubezpieczeń, Warszawa 2015, dr Piotr Majewski, PIU

ZWIĄZEK BANKÓW POLSKICH

Przetwarzanie i udostępnianie informacji objętych tajemnicami pomiędzy sektorem bankowym a sektorem ubezpieczeniowym

- Przykład 2

1. Osoba kierująca grupą wyszukuje auto po kolizji na serwisach aukcyjnych lub za granicą i „przepuszcza” je przez jeden z „zaprzyjaźnionych” autokomisów. Grupa współpracuje ponadto z kilkoma stacjami diagnostycznymi, które wydają zaświadczenia o przebytych przeglądach.

2. Wynajdowane są słupy, którym zostają udzielone kredyty na zakup przedmiotowych pojazdów. W tym osoby z grupy prowadziły własną działalność gosp. i rejestrowała takie osoby jako pracujące i wydawała zaświadczenia o zarobkach celem przedłożenia w banku.

3. Na zakup samochodu udzielany jest kredyt, a dwóch pracowników banku ściśle współpracuje z grupą.

4. Ubezpieczenia AC – osoby dostarczają zdjęcia innego pojazdu, odpowiednio przerobione przez informatyka.

5. Po 3–6 miesiącach od zakupu auto ginie (resztę kredytu spłaca ubezpieczyciel).

- *Analiza danych dotyczących przestępstw ujawnionych w 2014 r. w związku z działalnością zakładów ubezpieczeń – członków Polskiej Izby Ubezpieczeń, Warszawa 2015, dr Piotr Majewski, PIU

ZWIĄZEK BANKÓW POLSKICH

Przetwarzanie i udostępnianie informacji objętych tajemnicami pomiędzy sektorem bankowym a sektorem ubezpieczeniowym

- Art. 35a ustawy o działalności ubezpieczeniowej i reasekuracyjnej

Zakład ubezpieczeń może przetwarzać dane osobowe, w tym dane osobowe objęte obowiązkiem zachowania tajemnicy, o którym mowa w art. 35 ust. 1, w przypadku uzasadnionego podejrzenia popełnienia przestępstwa na szkodę zakładu ubezpieczeń w celu i zakresie niezbędnym do zapobiegania temu przestępstwu.

- Nowa regulacja – od 4.05.2019
- Nie wskazuje katalogu podmiotów, którym dane mogą zostać udostępnione
- Z uzasadnienia: *„W celu zapewnienia zakładom ubezpieczeń możliwości skutecznego zapobiegania przestępczości na ich szkodę (a w dalszej konsekwencji na szkodę ogółu ubezpieczonych) proponuje się uzupełnienie brzmienia art. 35 ustawy o działalności ubezpieczeniowej i reasekuracyjnej poprzez nadanie zakładowi ubezpieczeń uprawnienia do przetwarzanie informacji w przypadku uzasadnionego popełnienia przestępstwa na jego szkodę w celu i w zakresie niezbędnym do zapobiegania temu przestępstwu”.*

ZWIĄZEK BANKÓW POLSKICH

Konkluzje

- W związku z rosnącą liczbą zjawisk fraudowych, angażujących podmioty z różnych sektorów konieczne jest nawiązanie efektywnej współpracy międzysektorowej (chronimy tego samego klienta);
- Znacznym utrudnieniem przy efektywnym gromadzeniu danych oraz ich analizie są tajemnice sektorowe i brak możliwości zwolnienia z nich;
- Wymiana informacji przy wykorzystaniu Prokuratury/Policji z punktu widzenia sektora bankowego może być niewystarczająca ze względu na konieczność podjęcia działań w możliwie krótkim czasie (średni czas uchylania tajemnicy 2 tygodnie-2 miesiące).

ZWIĄZEK BANKÓW POLSKICH

Możliwości

- Opracowywanie dobrych praktyk wymiany informacji, nowych procedur, list kontaktowych, tworzenie relacji, systemów informatycznych;
- Dokonywanie zmian legislacyjnych – umożliwienie wymiany informacji pomiędzy sektorami w przypadku przestępstw lub uzasadnionych podejrzeń popełnienia przestępstw na szkodę podmiotów oraz ich klientów;
- Pozostajemy w kontakcie i prowadzimy dyskusję z sektorem telekomunikacyjnym oraz ubezpieczeniowym w celu wypracowania odpowiednich rozwiązań.

ZWIĄZEK BANKÓW POLSKICH

Dziękuję za uwagę

- monika.jozwiak@zbp.pl
- bcc@zbp.pl