Izba Domów Maklerskich

STANDARD IDM
W ZAKRESIE CYBERBEZPIECZEŃSTWA FIRM INWESTYCYJNYCH
W OBSZARZE STOSOWANIA
AKTYWNYCH LINKÓW I PROSTYCH HASEŁ

1. ZASADY OGÓLNE

Niniejszy Standard („**Dokument**") powstał w wyniku pracy grupy roboczej Izby Domów Maklerskich.

Przedstawiciele firm z sektora rynku kapitałowego biorących udział w pracach nad niniejszym dokumentem reprezentowali różne obszary biznesowe. W toku prac ustalono, że ze względu na stosowanie różnych modeli biznesowych przez firmy inwestycyjne oraz instytucje współpracujące z sektorem kapitałowym, w tym przez agentów firm inwestycyjnych, rekomendacje w niniejszym dokumencie będą koncentrowały się wyłącznie na aspektach bezpieczeństwa w obszarze stosowania aktywnych linków i prostych haseł.

Dokument przedstawia nadrzędne zasady rozumiane, jako wspólny standard dobrych praktyk, który powinien stanowić punkt odniesienia do wdrażania polityk bezpieczeństwa i szczegółowych procedur w ramach rozwiązań oferowanych przez poszczególne firmy z sektora kapitałowego.

Wyjaśnienie pojęć:

aktywne linki - to aktywne elementy wiadomości wysyłanych do klienta (tekst, przycisk, obrazek), które po kliknięciu uruchamiają zawartą pod nimi treść (strona, dokument etc.);

proste hasła – hasła utworzone na podstawie informacji, które można ustalić w ogólnie dostępnych źródłach (w rozumieniu listu Przewodniczącego KNF do sektora firm inwestycyjnych z 20 września 2021 r.);

tajemnica zawodowa – należy ją intepretować w szczególności w kontekście ustawy o obrocie instrumentami finansowymi.

Zasady nadrzędne:

1.1. Niniejszy Dokument został zainspirowany pismem: Cyberbezpieczeństwo elektronicznych kanałów dostępu do usług świadczonych przez firmy inwestycyjne - list Przewodniczącego KNF do sektora firm inwestycyjnych z 20 września 2021 r., w szczególności w kontekście obserwacji regulatora dotyczących praktyk stosowania przez podmioty regulowane aktywnych linków oraz tzw. „prostych haseł" w kanałach komunikacji z klientami.

1.2. Niniejsze rekomendacje i wytyczne należy traktować jako zbiór dobrych praktyk, których stosowanie powinno być poprzedzone analizą ryzyka przed wdrożeniem do stosowania konkretnych rozwiązań biznesowych.

1.3. Wyniki analizy ryzyka powinny być udokumentowane i cyklicznie aktualizowane.

1.4. Firmy Inwestycyjne oraz agenci firm inwestycyjnych, współpracujący z sektorem kapitałowym powinni wypracować i wdrożyć stosowne mechanizmy kontrolne, obejmujące etap wdrożenia i stosowania rekomendowanych rozwiązań wraz z ich udokumentowaniem.

1.5. Rekomendacje i zalecenia wskazane w Dokumencie, każda z instytucji z osobna wdraża adekwatnie do swojej sytuacji, w której identyfikuje rodzaje ryzyka wskazane w niniejszej samoregulacji.

1.6. Przytaczane rodzaje ryzyka nie stanowią katalogu zamkniętego, a jedynie te wymienione mają za zadanie określić przestrzeń zastosowania niniejszych rekomendacji i wytycznych.

1.7. Dla niektórych sytuacji stosowanie rozwiązania typu „proste hasła" jest najlepszym sposobem z punktu widzenia równoważenia bezpieczeństwa i konieczności poinformowania klienta o warunkach umowy lub sposobach jej wykonywania. Kwestie te powinny być przedmiotem analizy ryzyka w celu wypracowania spójnych zasad, uwzględniających m. in. ryzyko przełamania prostych haseł *versus* informacje i skutek ich ujawnienia w wyniku zastosowania omawianych metod ich zabezpieczenia.

2. REKOMENDACJE I WYTYCZNE

2.1. Ryzyko związane z brakiem jasnych, transparentnych dla klientów zasad dotyczących kanałów komunikowania się:

2.1.1. Zakres ryzyka

Brak świadomości klientów na temat stosowanych zasad, w zakresie wysyłania linków może wiązać się z:

2.1.1.1. Wchodzeniem przez klientów w interakcje z serwisami podszywającymi się pod instytucję finansową;

2.1.1.2. Brakiem pewności co do zakresu stosowanych standardów;

2.1.1.3. Podatnością na bycie zmanipulowanym;

2.1.1.4. Ryzykiem ujawnienia informacji wrażliwych;

2.1.1.5. Dezorientacją klienta co do zasad bezpieczeństwa stosowanych przez firmę inwestycyjną;

2.1.1.6. Brakiem zrozumienia zasad odpowiedzialności klienta firmy inwestycyjnej;

2.1.2. Rekomendacje ogólne

W ocenie firm inwestycyjnych przyjmujących Dokument, standardem powinno być:

2.1.2.1. Wprowadzenie do wysyłanej komunikacji informacji o możliwości zweryfikowania prawdziwości otrzymanej wiadomości poprzez kontakt z infolinią pod numerem prezentowanym w innym niezależnym przekazie (strona www, korespondencja listowna, inne treści edukacyjne);

2.1.2.2 W przypadku kontaktu z zewnątrz - weryfikacja po stronie klienta, czy dany konsultant pracuje we właściwej firmie inwestycyjnej;

2.1.2.3. Zachowanie spójności przekazu firmy inwestycyjnej do swoich klientów;

2.1.2.4. Stosowanie, tam gdzie to możliwe, opisowego nakierowania klienta do miejsca uzyskania informacji jakie otrzymałby poprzez kliknięcie w aktywny link.

2.1.3. Rekomendacje szczegółowe

W szczególności rekomenduje się wprowadzenie następujących rozwiązań:

2.1.3.1. Umieszczenie informacji na stronach www oraz w serwisie transakcyjnym komunikatu o stosowanych zasadach dotyczących linków w wiadomościach wysyłanych do klientów;

2.1.3.2. Treści przekazywanych informacji zawierają elementy zaufane (podpis cyfrowy, certyfikat) jednoznacznie identyfikujące nadawcę;

2.1.3.3. Przeprowadzenie kampanii informacyjnej o wprowadzeniu wykorzystania linków i standardów ich funkcjonowania;

2.1.3.4. Okresowe przypominanie klientom przyjętych zasad komunikowania się.

2.2. Ryzyko związane z ujawnieniem informacji chronionych w procesach komunikowania się z klientami.

2.2.1. Zakres ryzyka

2.2.1.1. Wysyłanie informacji prawnie chronionych z wykorzystaniem niezabezpieczonych środków komunikacji elektronicznej (e-mail, SMS, MMS) może prowadzić do ujawnienia tajemnic prawnie chronionych;

2.2.1.2. Wysyłanie linków prowadzących do serwisów transakcyjnych, autoryzacji transakcji, instalacji programów może prowadzić do wytworzenia nieprawidłowych nawyków wśród klientów, dla których podanie informacji wrażliwych na stronie, do której odsyła link powinno co do zasady być interpretowane jako usiłowanie wyłudzenia wrażliwych informacji;

2.2.1.3. Ryzyko wysłania wiadomości na adres lub numer telefonu, który nie należy do klienta

2.2.2. Rekomendacje ogólne

2.2.2.1. Firmy inwestycyjne powinny klasyfikować informacje przekazywane klientom co do zakresu przekazywanych treści i stosować do takich informacji odpowiednie do ryzyka ich ujawnienia standardy, w szczególności należy wyodrębnić:

- wszystkie załączniki wysyłane do klientów mailem zawierające dane osobowe lub informacje objęte tajemnicą zawodową;
- wszystkie niespersonalizowane załączniki wysyłane do klientów typu: regulaminy, wzorce umów/regulacje;

2.2.2.2. Informacje prawnie chronione (np. dane osobowe, tajemnica zawodowa) powinny być przesyłane do klientów przy zastosowaniu kanałów i metod, które pozwalają zapewnić tym informacjom adekwatne bezpieczeństwo (np. poczta wewnętrzna w internetowych kanałach firm inwestycyjnych lub oferowanych przez firmy inwestycyjne aplikacjach mobilnych, szyfrowanie wiadomości);

2.2.2.3. Firmy inwestycyjne powinny ustanowić zasadę, że w kanałach takich jak email lub SMS wysyłane są tylko informacje określonego typu np. marketingowe lub notyfikacyjne bez linków prowadzących do serwisów transakcyjnych, autoryzacji transakcji, instalacji programów itd.. Powyższa zasada nie jest stosowana w przypadku wykorzystania SMS jako drugiego składnika uwierzytelnienia;

2.2.2.4. Wiadomości e-mail do klientów powinny być podpisywane podpisem cyfrowym jednoznacznie identyfikującym instytucję jako nadawcę wiadomości (dopuszcza się sytuację, w której różne kategorie dokumentów będą podpisywane innym certyfikatem, wystawionym dla tej samej instytucji finansowej);

2.2.2.5. Zaleca się budowanie procesów, które mają możliwość weryfikacji poprawności adresu mailowego lub numeru telefonu klienta;

2.2.2.6. W komunikacji do klientów należy podkreślać wpływ zasad bezpieczeństwa stosowanych przez klienta dla zapewnienia poufności informacji, które otrzymuje lub wysyła oraz jego odporności na działania cyberprzestępców. Szczególną rolę w zapewnieniu bezpieczeństwa wymiany informacji między firmą inwestycyjną a klientem mają zasady ochrony przez klienta swojego dostępu do systemu transakcyjnego, konta pocztowego klienta oraz osobistych urządzeń komunikacyjnych, takich jak telefon, smartfon, tablet.

2.2.3. Rekomendacje szczegółowe

W szczególności rekomenduje się wprowadzenie standardów linkowania takich jak:

2.2.3.1. Nieużywanie linków prowadzących bezpośrednio do stron, które wymagają podania loginu, hasła lub innych wrażliwych oraz poufnych danych;

2.2.3.2. Nieużywanie linków prowadzących bezpośrednio do stron systemów transakcyjnych;

2.2.3.3. Nieużywanie usługi skracania długich linków do krótkiej formy przy użyciu ogólnodostępnych serwisów niezwiązanych z działalnością firmy inwestycyjnej (np. bit.ly/gHxGtx7a

2.2.3.4. Nieużywanie bezpośrednich linków w procesach nieinicjowanych przez klienta, prowadzących do stron umożliwiających bezpośrednie pobieranie oprogramowania;

2.2.3.5. Nieukrywanie adresu pod słowami kluczowymi lub grafiką CTA (Call To Action);

2.2.3.6. Zasady wskazane wyżej nie dotyczą stosowania linków w wewnętrznych kanałach komunikacyjnych dostępnych po przejściu procedury zalogowania do aplikacji mobilnej lub internetowych rozwiązań umożliwiających zalogowanie do systemu transakcyjnego firmy inwestycyjnej;

2.2.3.7. Informacje wysyłane do klientów pocztą elektroniczną, które zawierają dane osobowe lub informacje objęte tajemnicą zawodową, powinny być dodatkowo zabezpieczone tj. wysyłane jako zaszyfrowane załączniki do wiadomości, a treść samej wiadomości nie powinna zawierać informacji chronionych;

2.2.3.8. Jeżeli do zaszyfrowania załącznika zostało użyte hasło – to hasło do rozszyfrowania załącznika należy przekazać innym kanałem komunikacji (np. telefonicznie, SMS-em, przez portal umożliwiający klientowi dostęp do panelu transakcyjnego oferowanego przez firmę inwestycyjną, czy aplikację mobilną); hasło nie powinno być daną klienta łatwą do poznania typu numer PESEL, numer telefonu itp.; dopuszcza się zastosowanie hasła, które będzie daną znaną tylko obu stronom relacji klient/firma inwestycyjna (np. numer umowy brokerskiej czy numer rachunku klienta) lub kombinacją znaków, których ustalenie nie będzie łatwe do poznania przez osobę nieuprawnioną np. nazwiska panieńskiego matki w połączeniu z numerem dowodu osobistego lub paszportu; rekomenduje się umożliwienie klientowi ustawienie indywidualnego hasła z uwzględnieniem założeń dot. bezpieczeństwa konstrukcji hasła do załączników przekazywanych drogą mailową np. związane z

logowaniem się konta transakcyjnego dedykowanego klientowi lub innym kanale komunikowania się z klientem;

2.2.3.9. Dopuszcza się scenariusz, w którym hasło ustala klient, bądź firma inwestycyjna; klient ma prawo zmieniać hasło, które będzie stosowane wyłącznie do dokumentów wysłanych po jego zmianie.

2.2.3.10. Jeśli z jednego źródła klient otrzymuje kilka powiadomień, komunikat z hasłem powinien precyzyjnie określać, jakiego rodzaju wiadomości dotyczy i z jakiego okresu, w taki sposób, aby klient był w stanie dopasować hasła do zaszyfrowanych wiadomości.

2.3. STOSOWANIE MFA

2.3.1. Dostawcy usług finansowych powinni prowadzić monitoring związany z kwestiami cyberbezpieczeństwa i identyfikować obszary mogące stanowić zagrożenie dla klientów. Wieloskładnikowe uwierzytelnianie (MFA) powinno w szczególności obejmować kluczowe dla bezpieczeństwa klientów obszary.

2.3.2. Proces uwierzytelniania wieloskładnikowego polega na uzyskaniu od klienta dodatkowego poświadczenia jego tożsamości przy przeprowadzaniu określonych procesów związanych z jego rachunkiem inwestycyjnym. Jest to dodatkowe zabezpieczenie, stosowane łącznie z podaniem przez klienta loginu i hasła do systemu transakcyjnego.

2.3.3. Dodatkowe poświadczenie tożsamości może zostać zrealizowane m.in. za pomocą:
- 2.3.3.1. Kodu wysłanego poprzez SMS lub e-mail,
- 2.3.3.2. Kodu wysłanego kanałem powiadomień push,
- 2.3.3.3. Utworzenie przez klienta listy urządzeń zaufanych (autoryzacja urządzeń),
- 2.3.3.4. Sprzętowego urządzenia uwierzytelniającego (token),
- 2.3.3.5. Aplikacji uwierzytelniających.

2.3.4. Wieloskładnikowe uwierzytelnianie klienta powinno być stosowane w przypadku dokonywania kluczowych z punktu widzenia bezpieczeństwa czynności, w szczególności związanych z:
- 2.3.4.1. Wypłatą środków z rachunku klienta na inny niż zaufany (zdefiniowany przez klienta) rachunek bankowy;
- 2.3.4.2. Zmianą danych osobowych klienta;
- 2.3.4.3. Zmianą hasła dostępowego do rachunku inwestycyjnego, platformy transakcyjnej;
- 2.3.4.4. Zmianą danych kontaktowych: adresu e-mail, numeru telefonu, adres korespondencyjny;
- 2.3.4.5. Ustanowienie lub zmiana bankowego rachunku zaufanego;

2.3.5. W przypadku banku prowadzącego działalność w formie wyodrębnionego organizacyjnie biura maklerskiego, czynności opisane w niniejszym standardzie uznaje się za spełnione jeżeli bank stosuje wymogi silnego uwierzytelnienia klienta na podstawie ustawy o usługach płatniczych.

3. UDOKUMENTOWANIE STOSOWANYCH STANDARDÓW

3.1. Firmy inwestycyjne powinny stosować transparentne zasady komunikowania się z klientami. Zasady te powinny być udostępnione w taki sposób, aby zainteresowani klienci mogli łatwo się z nimi zapoznać.

3.2. Sposób zatwierdzenia i dokumentowania wprowadzonych zasad dotyczących komunikowania się powinien być zgodny z ładem korporacyjnym danej organizacji.

3.3. Udokumentowanie zasad oraz ich stosowanie powinno być przedmiotem wewnętrznych audytów, w celu zachowania spójności procesów w organizacji oraz zachowania jednolitego przekazu na zewnątrz, spójnego ze standardami przyjętymi na zasadach samoregulacji przez środowisko firm inwestycyjnych.