UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

Stanowisko
Urzędu Komisji Nadzoru Finansowego
w sprawie działań zakładów ubezpieczeń
i reasekuracji w zakresie cyberbezpieczeństwa

UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

Stanowisko Urzędu Komisji Nadzoru Finansowego w sprawie działań zakładów ubezpieczeń i reasekuracji w zakresie cyberbezpieczeństwa

Urząd Komisji Nadzoru Finansowego (dalej: Urząd Komisji, UKNF, organ nadzoru) obserwuje dynamiczny rozwój elektronicznych kanałów dostępu do usług świadczonych przez zakłady ubezpieczeń i reasekuracji (dalej: Zakłady), w którym nieprofesjonalni uczestnicy rynku przenoszą aktywność z tradycyjnych form kontaktu i współpracy z usługodawcami na rzecz kontaktu drogą elektroniczną. Oprócz oczywistych korzyści dla klienta, związanych z możliwością efektywnego zarządzania produktami ubezpieczeniowymi poprzez m.in. redukcję czasu i kosztów związanych z kontaktami z Zakładem, powszechność takiej formy świadczenia usług niesie za sobą również szereg ryzyk mających wpływ na bezpieczeństwo środków finansowych i danych klientów chronionych przepisami prawa, w tym tajemnicą ubezpieczeniową.

W ocenie Urzędu Komisji, mimo prowadzonych od wielu lat kampanii i działań edukacyjnych, których inicjatorami są m.in. podmioty rynku finansowego, obserwowana jest tendencja wzrostowa liczby nadużyć, których ofiarami są konsumenci korzystający z elektronicznych kanałów dostępu do usług finansowych. Dotyczy to zarówno osób aktywnie korzystających z nowoczesnych technologii i form komunikacji, jak i osób, które z takich kanałów korzystają sporadycznie.

Zasada „security first”

Podczas działań bieżących oraz w odniesieniu do działań planowanych, w szczególności w obszarze usług wykorzystujących elektroniczne kanały dostępu, Zakłady powinny konsekwentnie stosować paradygmat określany jako „security first”. Polega on na stawianiu bezpieczeństwa na pierwszym planie i podejmowaniu decyzji dotyczących kształtu procesów i produktów w oparciu o przeprowadzenie rzetelnych analiz ryzyka, które muszą uwzględniać nie tylko kwestie bezpieczeństwa środowiska teleinformatycznego Zakładu, ale również zagrożenia związane z korzystaniem z jego usług przez klientów. Potrzeby optymalizacji kosztowej czy procesowej, które mogłyby stanowić przyczyny reorganizacji sposobu prowadzenia działalności, nie mogą mieć wpływu na założenia i model tych analiz, zaś ich wyniki powinny być wykorzystywane do skutecznej kontroli ryzyka.

Analizy te powinny obejmować także wymagania wobec warunków świadczenia usług zdalnych, aby zapewnić maksymalny do osiągnięcia w danych warunkach poziom bezpieczeństwa środków finansowych i danych klientów oraz uwzględniać obecne trendy zagrożeń, wektory ataków na klientów, sposoby działań cyberprzestępców, a także potencjalne ryzyka wynikające z planowanych przez Zakład działań, nie tylko wobec swoich klientów, ale również w kontekście potencjalnego wpływu tych działań na cały sektor usług finansowych.

Wieloskładnikowe uwierzytelnianie w elektronicznych kanałach dostępu

W szczególności analizy te powinny również dotyczyć stosowanych przez Zakłady metod potwierdzania tożsamości klientów korzystających z elektronicznych kanałów dostępu. Wybór tych metod powinien być dokonywany z uwzględnieniem ryzyka związanego z tymi kanałami, w szczególności tego, czy i w jakim stopniu zastosowanie wieloskładnikowej weryfikacji tożsamości przyczyni się do zwiększenia poziomu bezpieczeństwa środków finansowych i danych klientów. Dotyczy to również zastosowania innych mechanizmów zabezpieczających, takich jak np. weryfikacja miejsca i czasu logowania do elektronicznego kanału dostępu oraz urządzenia, z którego takie logowanie ma miejsce. W opinii Urzędu Komisji, w obliczu zintensyfikowanych działań cyberprzestępców, brak stosowania silnego, wieloskładnikowego uwierzytelnienia klientów jest nieakceptowalnym ryzykiem. Takie uwierzytelnianie klienta powinno być stosowane w przypadku uzyskiwania przez użytkownika wglądu w informacje stanowiące tajemnicę ubezpieczeniową poprzez zdalne kanały dostępu Zakładu, jak również w sytuacji dokonywania przez klienta operacji związanych z zarządzaniem produktami ubezpieczeniowymi mogącymi nieść skutki finansowe, takimi jak ustalanie numerów rachunków bankowych lub realizacja transferów środków pieniężnych. Brak stosowania uwierzytelniania wieloskładnikowego w takich przypadkach może być dopuszczalny jedynie w sytuacji, gdy w wyniku przeprowadzonych analiz Zakład oceni, że ryzyko dla klienta jest niskie. Urząd Komisji oczekuje niezwłocznego podjęcia przez Zakłady prac mających na celu wdrożenie wieloskładnikowego uwierzytelnienia klientów w elektronicznych kanałach dostępu do usług Zakładów.

Unikanie aktywnych linków w komunikacji z klientami

Główną metodą ataków na klientów instytucji finansowych są działania socjotechniczne, wykorzystywane przez cyberprzestępców do podszywania się pod legalnie działające instytucje finansowe i inne organizacje, w celu pozyskania danych i poświadczeń klientów do logowania do elektronicznych kanałów dostępu, wykorzystywanych następnie do kradzieży danych lub środków finansowych. Przestępcze działania i ataki realizowane są poprzez wszystkie dostępne kanały komunikacji zdalnej, wykorzystywane również przez Zakłady do kontaktów z klientami, tj. kanał telefoniczny, wiadomości SMS, wiadomości e-mail oraz media społecznościowe, a działania te są na bieżąco dostosowywane przez przestępców do dynamicznie zmieniającej się rzeczywistości.

Od wielu lat zarówno instytucje finansowe, jak i organizacje działające na rzecz edukacji w zakresie cyberbezpieczeństwa, ostrzegają przed nierozważnym uruchamianiem linków otrzymywanych w wiadomościach SMS lub wiadomościach e-mail, zwracając uwagę na wysokie ryzyko poniesienia strat finansowych oraz ujawnienia i w konsekwencji przestępczego wykorzystania danych objętych tajemnicą ubezpieczeniową lub innych danych osobowych.

Prowadzone przez cyberprzestępców kampanie phishingowe, wykorzystujące SMS oraz wiadomości e-mail do rozsyłania linków internetowych, kierujących do fałszywych stron Zakładów bądź stron zawierających złośliwe oprogramowanie wykradające poświadczenia klientów do logowania do elektronicznych kanałów dostępu, mogą być źródłem poważnych strat finansowych klientów.

W związku z tym, organ nadzoru stoi na stanowisku, że wysyłanie aktywnych linków do stron internetowych w wiadomościach e-mail (włącznie z osadzaniem takich linków w grafikach) oraz wiadomościach SMS adresowanych do klientów, stoi w sprzeczności z tworzonym i od lat komunikowanym klientom przekazem związanym z ryzykiem utraty danych i środków finansowych, a Zakłady powinny dążyć do ograniczenia tej praktyki na rzecz informacji statycznych lub przekazywanych klientom poprzez aplikacje mobilne, lub inne kanały elektroniczne, które nie generują ryzyka oszustwa.

Zabezpieczenie komunikacji z klientami

Kolejnym istotnym czynnikiem ryzyka dotyczącym bezpieczeństwa środków finansowych i danych klientów, jest sposób zabezpieczania komunikacji z klientem, prowadzonej z wykorzystaniem poczty elektronicznej. Stosowane praktyki, polegające na zabezpieczaniu załączników przekazywanych w korespondencji e-mail prostymi czy krótkimi hasłami, składającymi się np. z fragmentów numeru PESEL klienta, kombinacji elementów numeru PESEL z datą urodzenia, numerem telefonu lub innymi hasłami, które są możliwe do odgadnięcia przy pomocy ogólnodostępnych narzędzi informatycznych w skończonym czasie, organ nadzoru uznaje za nieakceptowalne. Przekazywane w ten sposób informacje noszą znamiona informacji chronionych, bądź też zawierają dane osobowe, a budowanie prostych lub krótkich haseł jest sprzeczne z dobrymi praktykami w zakresie bezpieczeństwa.

Stosowana przez Zakłady forma komunikacji z klientem oraz przyjęte w tej komunikacji metody jej ochrony powinny być poprzedzone pogłębioną analizą ryzyka, ukierunkowaną na zabezpieczenie danych i informacji, uwzględniającą również aspekty użyteczności i jakości interakcji użytkownika z elektronicznymi kanałami dostępu (tzw. user experience). Analiza ta powinna obejmować stanowisko właściwej ds. cyberbezpieczeństwa komórki Zakładu, która będzie w stanie w rzetelny sposób ocenić, czy planowany sposób zabezpieczania korespondencji można uznać za bezpieczny. Niewłaściwe zabezpieczenie tych danych może być wykorzystane w celach przestępczych – np. do phishingu ukierunkowanego na konkretną osobę bądź grupę osób (spear phishing) – a także skutkować naruszeniem ochrony danych objętych tajemnicą ubezpieczeniową lub innych danych osobowych, narażając Zakład na

straty wizerunkowe oraz ryzyko nałożenia administracyjnej kary pieniężnej, na mocy art. 83 rozporządzenia 2016/679[1].

Mając na względzie potrzebę ograniczania niebezpiecznych z punktu widzenia organu nadzoru praktyk stosowanych przez Zakłady, korespondencja e-mail zawierająca załączniki, zwłaszcza z danymi objętymi tajemnicą ubezpieczeniową lub innymi danymi osobowymi, powinna być szyfrowana w sposób zapewniający poufność informacji, a odpowiednio długie i złożone hasło niezbędne do jej odszyfrowania powinno być przekazywane osobnym kanałem komunikacji, np. przez portal internetowy, aplikację mobilną lub SMS.

Umożliwienie klientowi ustawienia indywidualnego hasła do załączników przekazywanych drogą elektroniczną, uwzględniającego wskazane założenia i zgodnego z polityką haseł przyjętą przez Zakład bądź informacja o umieszczeniu załącznika w portalu, są rozwiązaniami, które mogą przyczynić się do pogodzenia potrzeby zapewnienia bezpieczeństwa informacji z wygodnym dostępem klienta do tych informacji. Takie rozwiązania, w ocenie Urzędu Komisji, przyczynią się do zwiększenia bezpieczeństwa danych klienta, bez zmniejszenia użyteczności zdalnych kanałów dostępu.

Kontrola nad działalnością zewnętrznych usługodawców

W tym kontekście organ nadzoru przypomina, że zgodnie z Wytycznymi Komisji Nadzoru Finansowego, dotyczącymi zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, wydanymi dla sektora ubezpieczeniowego, od Zakładów oczekuje się, że będą one sprawować skuteczną kontrolę także nad działalnością usługodawców zewnętrznych w zakresie świadczonych przez nich usług – zarówno podmiotów zewnętrznych wykonujących usługi na zlecenie Zakładów, jak i działających w imieniu lub na rzecz Zakładów pośredników ubezpieczeniowych. Kontrola ta powinna w szczególności dotyczyć stosowanych przez takich usługodawców mechanizmów kontrolnych i być realizowana albo poprzez ich weryfikację, wykonaną bezpośrednio przez Zakład, albo przegląd wyników weryfikacji tych mechanizmów kontrolnych realizowanych – np. z wykorzystaniem ogólnoświatowych standardów w tym zakresie, takich jak SSAE 16[2] – przez audyt wewnętrzny usługodawców lub niezależnych audytorów zewnętrznych.

[1] Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1 ze zm.)

[2] Statement on Standards for Attestation Engagements no. 16

Edukacja klientów

Świadomość w obszarze cyberbezpieczeństwa jest jednym z gwarantów bezpieczeństwa danych i środków finansowych klientów, a dbałość o jej budowanie powinna być przedmiotem szczególnej uwagi w komunikacji z klientami. Dotychczasowe działania w tym obszarze są w ocenie organu nadzoru niewystarczające. Budowanie świadomości klientów w zakresie cyberbezpieczeństwa nie powinno obecnie skupiać się wyłącznie na bezpieczeństwie korzystania ze zdalnych kanałów dostępu do usług ubezpieczeniowych i być prowadzone w formie ograniczonej do publikowania informacji na stronie internetowej Zakładu. Organ nadzoru zwraca uwagę, że ograniczenie się do działań edukacyjnych wykorzystujących Internet jako medium przekazu, prowadzi do ograniczenia lub pomijania pewnych grup konsumentów, co w konsekwencji skutkuje luką kompetencyjną w zakresie cyberbezpieczeństwa.

Wzmocnienie i konsekwencja działań w zakresie budowania świadomości klientów w obszarze cyberzagrożeń związanych z wykorzystaniem nowoczesnych technologii – w tym poprzez współpracę ze szkołami, środowiskiem akademickim i udział w kampaniach realizowanych przez instytucje konsumenckie – będzie miało bezpośrednie przełożenie na poziom bezpieczeństwa ich danych i środków finansowych. Takie działania edukacyjne korespondują z zaleceniami Rady Unii Europejskiej z 22 maja 2018 r. w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie[3], w których wskazuje się m.in. na udział czynnika biznesowego w kształtowaniu kompetencji cyfrowych społeczeństwa, charakteryzującego się krytycznym i odpowiedzialnym korzystaniem z technologii cyfrowych.

****

Działania Zakładów w zakresie cyberbezpieczeństwa, ze szczególnym uwzględnieniem aspektów wskazanych w piśmie oraz czynności podejmowanych w celu dostosowania działalności do wymagań nowo tworzonego rozporządzenia DORA[4], będą podlegały analizom i ocenom podczas czynności nadzorczych prowadzonych przez Komisję Nadzoru Finansowego – zarówno w zakresie postępowań inspekcyjnych, jak i analiz o charakterze systemowym.

[3] Zalecenia Rady z dnia 22 maja 2018 r. w sprawie w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie (2018/C 189/01) (Dz. Urz. UE C 189 z 4.06.2018, str. 1)

[4] Rozporządzenie Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014

Urząd Komisji Nadzoru Finansowego
ul. Piękna 20
00-549 Warszawa

www.knf.gov.pl