GAZETA FINANSOWA
15–21 czerwca 2018 r.

BEZPIECZNY BANK

Edukować pracowników i klientów – świadomość niebezpieczeństwa pozwala zachować ostrożność

Od pewnego czasu obserwujemy, że w cyberatakach dominują dwa główne trendy. W pierwszym przypadku przestępcy wykorzystują automatyzację do przeprowadzania ataków na szeroką skalę, w trakcie których ofiary nie są selekcjonowane. W drugiej sytuacji przeprowadzają tzw. ataki ukierunkowane, w których najpierw dokonują rekonesansu w środowisku organizacji, która jest ich celem, a następnie przedostają się do jej sieci.

Wojciech **Ciesielski**
menedżer Fortinet ds. klientów kluczowych sektora finansowego

Aby to osiągnąć, cyberprzestępcy wykorzystują różnego rodzaju zabiegi socjotechniczne, wśród których jednym z najpopularniejszych jest phishing – czyli wysłanie wiadomości e-mail z niebezpieczną zawartością w postaci załącznika lub linka. Tego typu ataki stają się coraz bardziej wyrafinowane, a przestępcy podszywają się na przykład pod pracowników wysokiego szczebla danej instytucji.

Odpowiednie narzędzia

Socjotechnika w atakach cyfrowych jest niestety wciąż skuteczna i będzie efektywna tak długo, jak pracownicy instytucji nie będą odpowiednio przeszkoleni w zakresie cyberbezpieczeństwa. Dotyczy to również pracowników sektora finansowego, a także przede wszystkim klientów instytucji finansowych, którzy zazwyczaj nie stosują odpowiednich narzędzi ochrony na komputerach i urządzeniach mobilnych. O ile instytucje finansowe stać na wdrażanie rozwiązań chroniących przed błędami pracowników, o tyle klienci są znacznie bardziej narażeni na atak i związane z nim straty finansowe.

Dla instytucji, jaką jest bank, groźna jest przede wszystkim sytuacja, kiedy cyberprzestępca przedostaje się do wewnętrznej sieci. Może powodować to szereg niebezpiecznych konsekwencji: od paraliżu działalności banku po kradzież danych lub środków finansowych. Każdy z tych przypadków rzutuje na dalsze funkcjonowanie instytucji i ma nie tylko łatwo mierzalne finansowo skutki. Może powodować również spadek zaufania, które w finansach jest szczególnie ważne, a w dalszej konsekwencji – utratę klientów i kłopoty z prawem, np. związane z ochroną danych podlegających ochronie.

Zaplanować środki na edukację

Biorąc pod uwagę powyższe argumenty, zarządy instytucji finansowych powinny zaplanować odpowiednie środki przeznaczone na edukację personelu. Naruszeń bezpieczeństwa związanych z atakami socjotechnicznymi można stosunkowo łatwo uniknąć. Właściwie przeszkoleni pracownicy powinni mieć świadomość, aby w żadnym wypadku nie otwierać załączników od nieznanych nadawców e-maili oraz nie klikać w podejrzane linki, nawet jeśli są one przesyłane od znanych im osób.

Warto przy tym pamiętać, że zachowywanie cyberhigieny przez personel powinno być wsparte odpowiednimi rozwiązaniami sprzętowymi i oprogramowaniem. Ważne jest także przeprowadzanie regularnych testów penetracyjnych, które mogą ujawnić istniejące luki w bezpieczeństwie. Czynnik ludzki zawsze będzie jednak najsłabszym ogniwem architektury zabezpieczeń.

Jeśli chodzi o relacje z klientami, to każdy bank powinien mieć opracowany system szybkiego informowania użytkowników o nowo pojawiających się zagrożeniach i o tym, jak się ich wystrzegać. To właśnie zdolność systemu do szybkiego reagowania na incydenty jest kluczowa w zapobieganiu skutkom ataku.

Czujny klient

Ponadto użytkownicy powinni być przez bank edukowani w zakresie bezpiecznego korzystania z usług online. Cyberprzestępcy najczęściej uciekają się do oszustwa, wysyłając maile do złudzenia przypominające oficjalne wiadomości od banku. Zawarty w nich złośliwy załącznik pozwala po uruchomieniu na przechwytywanie wrażliwych informacji, jak np. dane logowania. Hakerzy tworzą też atrapy serwisów bankowych, które bazują na wyglądzie oryginalnych stron.

Klienci powinni więc każdorazowo zwracać uwagę na to, czy w pasku adresu przeglądarki widnieje prawidłowa nazwa domeny ich banku rozpoczynająca się od https. Standardem powinno być ustawienie dwuetapowej weryfikacji dostępu do konta, w której, poza podaniem hasła podczas logowania, konieczne będzie również wpisanie np. kodu SMS otrzymanego od banku.

W kształtowaniu świadomości klientów ważną rolę mogą odegrać też zrzeszenia i organizacje branżowe sektora finansowego oraz władze państwowe, co jest szczególnie ważne z punktu widzenia trwającej transformacji cyfrowej i budowania społeczeństwa cyfrowego. Zaufanie do nowych cyfrowych usług finansowych jest też kluczem do rozwoju rynku bezgotówkowego.

Jak nowoczesny Customer Experience wpływa na wzrost sprzedaży i detekcję fraudów

Badania rynkowe dowodzą, że instytucje finansowe na całym świecie kierują swoją uwagę na Customer Experience, a firmy mierzące ROI, uwzględniając CX notują w 50 proc. wzrost nie tylko satysfakcji i lojalności swoich klientów, ale przede wszystkim wzrost sprzedaży i większą konwersję leadów.

Michał **Góra**
członek zarządu Alfavox

W dobie wzmożonej cyberprzestępczości, bezpieczeństwo staje się priorytetem placówek bankowych, a eksperci zastanawiają się, gdzie leży punkt równowagi między optymalnym poziomem bezpieczeństwa i przyjaznym dla klienta Customer Experience. Czy to oznacza konieczność rezygnacji z usability, podczas gdy fraudy generują straty rzędu 70 mld $ a tradycyjne metody, takie jak hasła czy kody PIN, nie gwarantują już wystarczającej ochrony? Rozwiązaniem jest zastosowanie biometrycznej video identyfikacji, która natychmiast przekłada się na wzrost Customer Experience oraz wzrost biznesu.

Customer Experience coraz częściej decyduje o sukcesie marki. Wpływa na takie wskaźniki pomiaru rozwoju firmy jak: wartość przychodów, czas finalizacji transakcji czy indywidualne rezultaty managerów. Z badania przeprowadzonego w 2018 roku pośród największych firm świata działających w branży finansowej wynika, że 93 proc. organizacji mierzących ROI potwierdza, iż dzięki realizacji i monitorowaniu działań Customer Experience wzrastają wskaźniki satysfakcji klienta czy NSP (Net Promoting Score), a w 50 proc. organizacji wzrastają również dochody firmy.

W biznesie nie liczy się tylko sam wzrost sprzedaży. Chodzi o to, by robić to mądrze. Należy bowiem pamiętać, że w bankowości cały czas trwa wyścig. Wyścig przede wszystkim o klienta, jego zaufanie i lojalność. Szybkość jest w nim siłą napędową sprzedaży. Szybkość obsługi klienta, szybkość dotarcia do niego czy wreszcie szybkość autoryzacji. Dla instytucji bankowych szczególnie ważne jest posiadanie narzędzia, które w realny sposób zagwarantuje szybką obsługę przy wysokiej skuteczności wykrywania prób nadużyć finansowych. Analiza wiarygodności dokumentacji i weryfikacja dokumentu tożsamości to procesy wymagające czasu, dlatego stają się punktem zwrotnym w tym wyścigu. Odpowiedzią jest biometryczna video weryfikacja, która gwarantuje spełnienie najwyższych norm bezpieczeństwa z jednoczesnym zachowaniem wysokich standardów obsługi, oczekiwanych od instytucji bankowych. Klienci otrzymują gwarancję poufności i ochrony swoich danych oraz mogą wygodnie zrealizować operacje finansowe w krótkim czasie. Jest to szczególnie istotne w obliczu rosnącej ilości cyber fraudów i perspektywy, że do 2020 roku aż 75 proc. firm, które używają wielu kanałów komunikacji z klientami, poniesie straty spowodowane przez cyberprzestępców. Jednocześnie w tym czasie zaledwie 30 proc. firm będzie stosowało zintegrowane, wielokanałowe rozwiązania, skutecznie wpływające na detekcję i zapobieganie fraudom.

Ogromne skutki rosnącej defraudacji

Wyciek danych klientów czy spadek zaufania do instytucji to tylko niektóre konsekwencje fraudów. Dotkliwe są też straty finansowe, które w 2014 roku sięgały 70 mld USD, a w 2016 roku, w samej tylko Wielkiej Brytanii przekroczyły 1 mld $. Niepokoi przy tym dynamika wzrostu cyber fraudów, dla przykładu w 2014 roku liczba instytucji, które zanotowały straty w wysokości między 10 mln USD a 22 mln USD wzrosła o 150 proc. w stosunku do roku poprzedniego.

(Nie)bezpieczne hasła

Powodem rosnącej defraudacji jest często słabość dotychczasowych zabezpieczeń. Jak wynika z badań, do 2022 roku liczba wizyt w oddziałach tradycyjnych banków spadnie jeszcze o blisko 70 proc. Bankowość elektroniczna i technologia wideo wypierają dotychczasowy model kontaktu z klientami. Wymusza to na instytucjach potrzebę wysokiej jakości uwierzytelniania dokumentacji oraz weryfikacji tożsamości swoich klientów. Choć dwupoziomowe hasła gwarantują wyższe bezpieczeństwo danych, nie są powszechnie stosowane ze względu na Customer Experience i wygodę użytkowników. To pogarsza wskaźniki konwersji i sprzedaży. I choć zabezpieczanie dostępu hasłem nadal jest najpopularniejszym rozwiązaniem, najnowsze raporty pokazują, że hasła nie gwarantują już 100 proc. bezpieczeństwa i stają się bezużyteczne w przypadku wielu nowych typów nadużyć. Już sam fakt, że w 2016 roku zgłoszono kradzież 3 mld danych użytkowników, a blisko 59 proc. klientów posługuje się tym samym hasłem podczas korzystania z różnych usług sprawia, że instytucje finansowe powinny zainwestować w nowocześniejsze rozwiązania gwarantujące cyberbezpieczeństwo.

Inwestycje w bezpieczeństwo

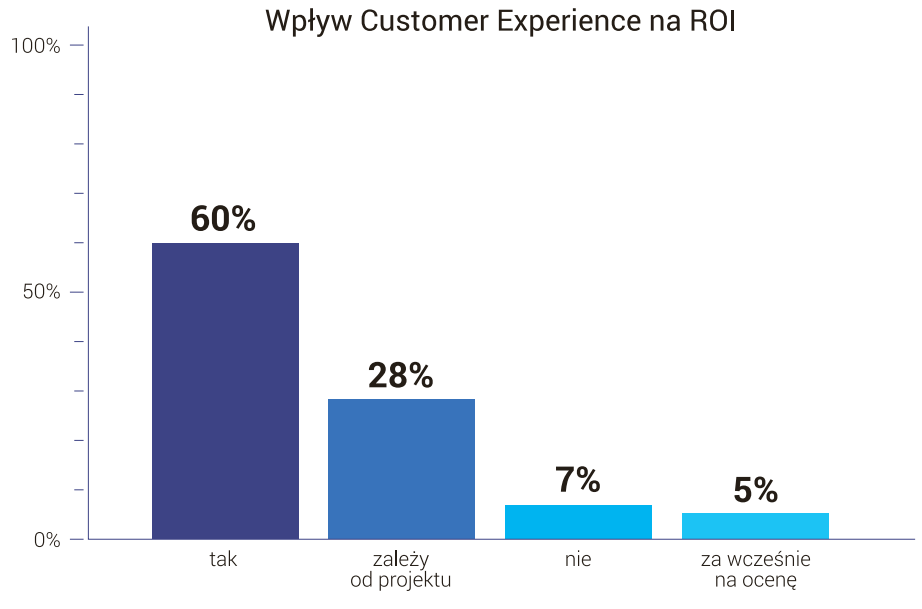
Z badań prowadzonych przez globalne firmy analityczne wśród dyrektorów CEO i CTO w instytucjach finansowych, wynika, że firmy te alokują coraz większe budżety w rozwiązania nowej generacji, które wzmocnią lub nawet całkowicie wyeliminują przestarzałe narzędzia uwierzytelniania. Skalę działań doskonale obrazuje zapowiedziane przez Lloyd's Bank zwiększenie do 4 mld $ nakładów na inwestycje w rozwiązania typu customer centric, low risk. Nadszedł zatem czas, aby pracownicy działów bezpieczeństwa, zainteresowali się zabezpieczeniami biometrycznymi z co najmniej dwóch powodów.

Po pierwsze, metody autoryzacji biometrycznej, stosowane samodzielnie lub w połączeniu z tradycyjnymi metodami, np. hasłami lub nr PIN, zwiększają bezpieczeństwo. Przy czym jak wynika z raportu „Technology Insight for Biometric Authentication" już w 2020 roku w przedsiębiorstwach stosujących zabezpieczenia biometryczne aż 70 proc. będzie opierało się na łączeniu rozpoznawania twarzy czy głosu z metodami „pasywnymi". Po drugie, stosowanie zabezpieczeń biometrycznych wpływa na komfort i zadowolenie klientów, którzy nie muszą pamiętać haseł (lub korzystać z programów do ich gromadzenia) ani też nosić ze sobą karty kredytowej, żeby podać jej numer czy kody CVV, CVC.

Biometryczna video identyfikacja Alfavox przyszłością bezpiecznej bankowości

Wzrost skuteczności wykrywania fraudów o 78 proc., optymalizacja procesów weryfikacji tożsamości i 2-krotne skrócenie czasu potrzebnego do zawarcia umowy to rezultat, który mogą osiągnąć instytucje finansowe wykorzystując rozwiązanie biometrycznej video weryfikacji. O tym, że takie rozwiązania skutecznie zwiększają bezpieczeństwo przekonuje Alfavox, producent rozwiązań Customer Experience, w tym przełomowego systemu biometrycznej video weryfikacji, docenionego nagrodą w tegorocznej edycji konkursu «Hit Roku» 2018 dla instytucji finansowych. Dzięki systemowi, który opiera się na użyciu zaawansowanych modułów biometrycznych, możliwa jest zdalna i automatyczna weryfikacja dokumentu tożsamości oraz identyfikacja twarzy klienta w kanale video. Rozwiązanie to pozwala na bezpieczne uwierzytelnienie klienta w zaledwie kilka sekund. Moduł video identyfikacji sprawdza dane biometryczne, poprawność, integralność i oryginalność dokumentu okazanego przez klienta. System weryfikuje numer dokumentu oraz numer PESEL, jednocześnie sprawdzając bazy zgubionych i skradzionych dokumentów, prowadząc w ten sposób do wzrostu wskaźnika wykrywalności fraudów o 78 proc. Proces obsługi klienta zostaje przy tym skrócony 2-krotnie co wpływa korzystnie na budowanie pozytywnych relacji między klientami a marką oraz podkreśla innowacyjny i nowoczesny wizerunek instytucji na rynku. Teraz konto online można otworzyć zaledwie w 5 minut, z dowolnego miejsca, bez planowania wizyty w placówce banku czy wykonywania przelewu weryfikacyjnego z innego banku.

Dzięki takim rozwiązaniom lojalność klientów rośnie, firmy doskonalą Customer Experience, a ich sprzedaż rośnie. Jeśli zatem zadbamy o stały wzrost usability zyskamy niepowtarzalną wartość. Będzie to unikalna przewaga konkurencyjna, która zapewni firmie stały rozwój biznesu.



Wyniki badania przeprowadzonego w 2017 roku na grupie 160 firm na świecie potwierdzają, że organizacje dbające o CX odnotowują znaczące zwroty z inwestycji.

BEZPIECZNY BANK

Liczą się bezpieczeństwo i zaufanie

Współcześni klienci banków oczekują od instytucji finansowych szerszego wykorzystania technologii i świadczenia innowacyjnych usług. Jednocześnie jednak nadal chcą odwiedzać stacjonarne oddziały zlokalizowane jak najbliżej domu.

Badanie Salesforce ujęte w raporcie „2017 Connected Banking Customer Report" poświęcono trendom na rynku usług finansowych i oczekiwaniom klientów. Jak pokazuje badanie, im mniej innowacyjnych i użytecznych usług oferuje bank, tym częściej klienci korzystają z oferty firm fintech, co zaburza dotychczasowy status quo na rynku detalicznych usług bankowych. Klienci oczekują m.in. takich udogodnień, jak wirtualne oddziały, blockchain, obsługa walut cyfrowych, voice banking czy roboty pełniące rolę kasjerów i doradców.

Technologie zmieniają rynek i wymuszają konkurencyjność

Cyfrowa transformacja ma ogromy wpływ na sektor finansowy nie tylko dlatego, że wymaga od tradycyjnych banków przekładania nowych technologii na innowacyjne usługi. Jedną z konsekwencji transformacji cyfrowej jest również pojawienie się tzw. firm fintech (financial technology), które oferują usługi dotąd świadczone wyłącznie przez instytucje finansowe. Aby nie stracić kawałka rynkowego tortu, banki detaliczne muszą więc stawać się bardziej konkurencyjne.

Badanie Salesforce „2017 Connected Banking Customer Report" przeprowadzone na grupie klientów banków z USA i Wielkiej Brytanii wykazało, że rosnąca ilość firm fintech zaburza rynek bankowości detalicznej. Coraz więcej klientów korzysta z usług nowych firm podczas dokonywania różnego rodzaju płatności i jest to tendencja widoczna we wszystkich grupach wiekowych. Pomimo iż banki oferują podobne usługi, klienci wybierają ofertę fintech z powodu wygody oraz łatwości używania ich rozwiązań. Banki stoją więc przed ważnym momentem, jakiego jeszcze w tej branży nie było: jeśli nie chcą zmniejszenia swoich udziałów w rynku, muszą postawić na innowacyjność i walkę o klienta, zwłaszcza w obszarach, które zaczęły obsługiwać fintechy.

Klient wybiera bezpieczeństwo i zaufanie

Ostatnie zmiany polityczne i gospodarcze, takie jak wybory prezydenckie w USA i Brexit wyraźnie wpłynęły na klientów banków. W niespokojnych czasach znaczenie zaufania i bezpieczeństwa danych wzrosło wśród klientów. Średnio dwie trzecie Amerykanów uznaje, że finansowa stabilność banku (63 proc.) i bezpieczeństwo danych osobowych (66 proc.) są najważniejszymi czynnikami wyboru banku, w którym ma być prowadzone konto osobiste. Co ciekawe, chociaż większość ufa informacjom podawanym przez banki, to jednak tylko 26 proc. uznaje, że dobro klienta jest tam najwyższym priorytetem. Jak widać w dziedzinie zaufania wiele jest do nadrobienia.

Triumf mobilnej bankowości i przywiązanie do fizycznych oddziałów

Rutynowe transakcje bankowe (wpłaty, wypłaty, depozyty), jakich dokonują dzisiejsi klienci w USA, realizowane są zarówno zdalnie, jak i w oddziałach. Ponad 30 proc. takich operacji wykonywanych jest za pośrednictwem serwisu internetowego, 16 proc. za pomocą aplikacji mobilnych, 12 proc. w bankomatach. Wciąż jednak 21 proc. klientów korzysta po prostu z kasy w oddziale banku.

Największy wzrost odnotowuje obecnie bankowość mobilna. Jedna trzecia klientów (31 proc.) z najmłodszej grupy wiekowej posiadających konta bieżące lub oszczędnościowe, wykorzystuje bankowe aplikacje mobilne do większości rutynowych transakcji. Chociaż banki ułatwiają wykonywanie transakcji poprzez urządzenia mobilne, duża grupa klientów (niezależnie od wieku) kontynuuje wizyty w stacjonarnych oddziałach. Aż 58 proc. Amerykanów odwiedza oddział swojego banku raz w miesiącu. Ten trend jest korzystny dla banków tradycyjnych, dając przewagę konkurencyjną nad wirtualnymi fintechami, które takiej opcji nie posiadają. Likwidacja oddziałów bankowych (lub ich znaczące ograniczenie) prognozowana przez analityków nie nastąpi więc zapewne tak szybko, jak się spodziewano – przynajmniej w USA. Wśród amerykańskich klientów, którzy w ciągu ostatnich 5 lat zmienili bank, 39 proc. wybrało tradycyjny, duży bank krajowy, a tylko 13 proc. najmłodszych – bank cyfrowy dostępny wyłącznie w sieci. Jednym z najważniejszych kryteriów wyboru okazała się bliska odległość oddziału od miejsca zamieszkania. Był to czynnik równie istotny jak bezpieczeństwo danych, łatwe w użyciu aplikacje mobilne, większe możliwości transakcji online, nowoczesne technologie w oddziałach fizycznych (tablety, digital signage, beacony) czy personalizacja obsługi.

Amerykańskie fintechy przejmują klientów banków

W Stanach Zjednoczonych klienci banków nadal nie uważają branży bankowej za innowacyjną, w przeciwieństwie do takich sektorów jak: prywatna ochrona zdrowia czy handel detaliczny. To właśnie braki banków tradycyjnych w dziedzinie innowacyjnego zastosowania technologii wykorzystały fintechy, oferując nowocześniejsze usługi finansowe, które cieszą się coraz większą popularnością. Płatności za ich pośrednictwem dokonuje już 83 proc. ludzi z pokolenia Millenialsów (18-34 lata), aż 79 proc. z pokolenia X (35-54 lata) i 62 proc. z pokolenia Baby Bomers (+55 lat). Jeszcze bardziej wymowny jest fakt, że 55 proc. najmłodszych klientów woli przeprowadzać transakcje za pośrednictwem fintech, niż przy użyciu podobnych usług oferowanych przez banki, ponieważ uważają je za wygodniejsze (56 proc.), szybsze i łatwiejsze w obsłudze (55 proc.).

Z badania Salesforce wynika, że klienci banków detalicznych zdecydowanie rzadziej kierowaliby swoją uwagę w stronę fintechów, gdyby ich banki oferowały innowacyjne rozwiązania, takie jak: wirtualne oddziały, możliwość dokonywania operacji za pomocą głosu (mówienie do aplikacji w telefonie), obsługę walut cyfrowych (np. bitcoin), usługi peer-to-peer, wykorzystanie sztucznej inteligencji w postaci robotów w roli kasjerów czy doradców finansowych. Klienci chcieliby również, by banki w celu zapewnienia bezpieczeństwa danych i transakcji stosowały technologię blockchain (zbiorowa, cyfrowa księga rachunkowa transakcji rozproszona po całej sieci, w takich samych kopiach). Technologia ta opiera się na sieci peer-to-peer bez centralnych komputerów, systemów zarządzających i weryfikujących transakcje).

Młodzi Brytyjczycy wątpią w innowacyjność banków i wybierają fintechy

Podobnie jak Amerykanie, klienci w Wielkiej Brytanii kontynuują wizyty w oddziałach swoich banków, pomimo posiadania dostępu do usług internetowych: 41 proc. odwiedza swój bank przynajmniej raz w miesiącu, a 32 proc. robi to raz na kilka miesięcy. Do wykonywania rutynowych działań na koncie używają głównie strony internetowej (30 proc.), kasy w oddziale (21 proc.), aplikacji mobilnych (15 proc.) i bankomatu (10 proc/).

Co do innowacyjności brytyjskich banków zdania są podzielone. Aż 58 proc. klientów z pokolenia X uważa, że są one tak samo innowacyjne jak branża prywatnej ochrony zdrowia, handel detaliczny czy sektor nowych technologii. Jednak najmłodsi klienci nie mają dobrego zdania o nowoczesności brytyjskich banków – za takie uznaje je jedynie 10 proc., podczas gdy 43 proc. uważa, że ich bank używa przestarzałych technologii (np. nie posiada aplikacji mobilnych).

Podobnie jak w USA, brytyjscy Millenialsi (52 proc.) i pokolenie X (33 proc.) z powodu braku nowoczesnych narzędzi w swoich bankach wolą używać do podstawowych płatności usług firm fintech, ponieważ alternatywne rozwiązania oferowane przez ich bank oceniają znacznie słabiej.

Polski klient banku ma dostęp do najnowocześniejszych usług

W Polsce sytuacja jest dość specyficzna, ponieważ polskie banki są w gronie liderów zmian technologicznych na świecie. W ostatnich kilku latach zdobyły one 24 nagrody w 12 międzynarodowych konkursach (m.in. Best of Show, Model Bank Awards). Polscy klienci, szczególnie młodsze pokolenia, są więc przyzwyczajeni do korzystania z nowoczesnych rozwiązań, co spowodowało, że staliśmy się liderem w dziedzinie płatności zbliżeniowych. Obecnie aż 55 proc. wszystkich płatności kartą w Polsce jest przeprowadzonych bezstykowo.

Innym przykładem szybkiej adaptacji nowości technologicznych jest bankowość mobilna. Jak wynika z raportu PwC „Sektor finansowy coraz bardziej #fintech", aż 61 proc. posiadaczy komórek w Polsce używa aplikacji mobilnej, co jest najwyższym wynikiem w Unii Europejskiej (przy średniej 40 proc.). Polski klient jest jeszcze pod jednym względem specyficzny – jest najmniej przywiązany do swojego banku i najczęściej zmienia bank główny, przenosząc się tam, gdzie otrzymuje nowocześniejsze niż uprzednio rozwiązania.

Wszystko to sprawia, że sytuacja fintechów w Polsce jest odmienna niż w innych krajach. Fintechy, które muszą się mierzyć z bankami będącymi liderami innowacji, zamiast trudnych zmagań na rynku często stawiają na współpracę, co jest korzystne dla wszystkich stron. Według badania Monitora Bankowego z 2016 roku, bankowcy określają firmy fintech jako inspirację do wprowadzania nowych produktów (75 proc.) oraz sugerują, że mogą to być potencjalni partnerzy innowacji (66 proc.). Tylko 51 proc. badanych w Polsce instytucji finansowych obawia się, że firmy te niosą ryzyko przejęcia dotychczasowych klientów.

Nie oznacza to jednak, że banki w Polsce mogą spać całkiem spokojnie. Muszą pilnować obszarów najbardziej zagrożonych konkurencją ze strony fintechów, a należą do nich: bankowość indywidualna, przekazy pieniężne i płatności, inwestycje i zarządzanie aktywami, bankowość dla małych i średnich firm oraz usługi brokerskie.

Sytuację na rynku usług finansowych w Europie zmienią zapewne nowe przepisy regulacyjne, czyli PSD2 (Dyrektywa Parlamentu Europejskiego i Rady Unii Europejskiej 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego), która wprowadza na rynek płatności nową kategorię podmiotów – dostawców usług płatniczych, będących osobami trzecimi TPP – third party provider. PSD2 wpłynie w znaczącym stopniu na kształt całego rynku usług płatniczych i ułatwi rozwój fintechów.

Fuzje i przejęcia a cyberbezpieczeństwo

Fuzje i przejęcia (ang. Mergers & Acquisitions – M&A) to dla przedsiębiorstw jedne z najbardziej ryzykownych operacji. Nie tylko pod względem finansowym. Niosą ze sobą również ogromne ryzyko dla cyberbezpieczeństwa firmy. Firmy cały czas narażone są na ataki ze strony cyberprzestępców, ale sprawa komplikuje się, gdy dochodzi do nich podczas procesu fuzji lub przejęcia przedsiębiorstw. Czy organizacje przed dokonaniem transakcji nie powinny zatem wziąć pod uwagę kwestii takich jak procedury bezpieczeństwa? A co z zagrożeniem bezpieczeństwa pracowników, którzy w wyniku M&A tracą pracę? Co dzieje się z personelem ds. bezpieczeństwa, gdy umowa zostanie już zawarta?

Co budzi największe obawy?
Na początku 2017 roku, West Monroe Partners przeprowadziło badanie, które skoncentrowane było na fuzjach i przejęciach w sektorze oprogramowania. Przebadano 100 światowych przedstawicieli kadry kierowniczej i okazało się, że cyberbezpieczeństwo jest kwestią budzącą poważne obawy – zarówno w trakcie, jak i po zakończeniu procesu M&A. Ponad połowa respondentów (52 proc.) odkryła problemy z cybebezpieczeństwem już po zakończeniu transakcji, a znacznie więcej było niezadowolonych z przeprowadzanych audytów bezpieczeństwa cybernetycznego. Raport wykazał również, że problemy z cyberbezpieczeństwem były drugim w kolejności powodem odstąpienia od umowy. To również przez problemy z cyberbezpieczeństwem wielu respondentów żałowało decyzji o fuzji lub przejęciu innego przedsiębiorstwa.

Jak zadbać o cyberbezpieczeństwo firmy podczas fuzji lub przejęcia?
Wyzwanie dotyczące zabezpieczeń, przed którym stoją przedsiębiorstwa podczas M&A jest o tyle większe, że wciąż brakuje wykwalifikowanych ekspertów ds. bezpieczeństwa. Firmy biorące pod uwagę tego typu transakcje powinny rozważyć kilka dobrych praktyk, które pomogą rozwiązać zagrożenia.

- Pierwsza polega na dokładnym przeanalizowaniu i zrozumieniu systemu zabezpieczeń organizacji. Chodzi tu m.in. o nierozwiązane kwestie bezpieczeństwa, zgłoszone naruszenia oraz jakiekolwiek inne nieprawidłowości w tym zakresie. Kluczowy jest gruntowny audyt wszystkich polityk i procedur bezpieczeństwa oraz spotkanie z kadrą kierowniczą odpowiedzialną za bezpieczeństwo przedsiębiorstwa.
- Inną dobrą praktyką jest skorzystanie z usług firmy zewnętrznej, która przeprowadzi kwestionariusz wśród pracowników bezpieczeństwa IT docelowej firmy. Jest to sposób na zidentyfikowanie najbardziej strategicznych zasobów informacyjnych, jakie posiada firma (własność intelektualna i dane klientów), a także sprawdzenie, gdzie przechowywane są informacje oraz jak są one chronione.
- Bardzo ważne jest również upewnienie się, że komunikacja wewnętrzna działa sprawnie i pracownicy firmy są na bieżąco informowani o zagrożeniach takich jak złośliwe oprogramowanie, ransomware i phishing.
- W przypadku przejęcia, firma nabywająca musi dokonać oceny polityk bezpieczeństwa obu przedsiębiorstw i naprawić wszystkie wykryte w zabezpieczeniach luki. Jeśli chodzi o fuzję, to każda z firm powinna sprawdzić i porównać swoje systemy bezpieczeństwa oraz wprowadzić niezbędne zmiany.

Sz/ma/Bitdefender

Coraz więcej ataków ukierunkowanych

Według badania przeprowadzonego przez firmę F-Secure aż 55 proc. incydentów wykrytych w przedsiębiorstwach stanowią ataki ukierunkowane. Hakerom coraz częściej udaje się przeprowadzić cyberatak, któremu nie są w stanie zapobiec tradycyjne rozwiązania do zabezpieczania urządzeń końcowych (komputerów Windows i Mac, smartfonów czy platform serwerowych). – Cyberprzestępcy stosują coraz bardziej wyszukane metody, aby przeprowadzić atak, a to z kolei wymaga nowatorskiego podejścia do kwestii ochrony. Na rynku cyberbezpieczeństwa brakuje specjalistów. Ataki ukierunkowane coraz częściej wymierzone są w firmy średniej wielkości, a te nie są w stanie ponieść wysokich kosztów zatrudnienia pracowników dedykowanych wyłącznie kwestiom bezpieczeństwa IT – mówi Magdalena Baraniewska, Country Channel Manager w firmie F-Secure.

BIK W CYFROWEJ PRZESTRZENI

Biuro Informacji Kredytowej, kojarzone powszechnie jako instytucja finansowa, jest również nowoczesną firmą technologiczną. BIK to największy zbiór danych w Polsce, pochodzących z całego sektora bankowego zarówno o klientach indywidualnych i przedsiębiorcach, a także z obszaru pożyczek pozabankowych, stanowiący informację o 148 mln rachunków należących do 24,3 mln klientów indywidualnych oraz informację o historii kredytowej łącznie 1,2 mln firm, rolników i innych podmiotów, w tym o 757 tys. mikroprzedsiębiorców prowadzących działalność gospodarczą. BIK, współpracując oraz wspierając sektor bankowy i pożyczkowy, dostarcza wiele rozwiązań technologicznych. Na bieżąco obserwuje i aktywnie wdraża najlepsze nowatorskie rozwiązania informatyczne. Ostatnio mocno widoczne jest zaangażowanie BIK zwłaszcza w dwóch nowych obszarach rozwiązań technologicznych: w technologii blockchain i systemach antyfraudowych.

Odnaleźć się w zdigitalizowanej gospodarce

Agnieszka Szopa – Maziukiewicz dyrektor zarządzający Obszarem IT, BIK

W zdigitalizowanej gospodarce, gdzie większość transakcji zawieranych jest online w ułamkach sekund, technologia blockchain ma duży potencjał zrewolucjonizowania bankowości pod względem efektywności, bezpieczeństwa oraz wiarygodności. Pewność transakcji, niezmienność ich potwierdzenia, pełna audytowalność wszystkich operacji budują zaufanie między stronami. Te wszystkie cechy posiada technologia blockchain firmy Billon z wykorzystaniem której BIK przygotowuje rozwiązanie do przechowywania i wymiany dokumentów pomiędzy instytucjami a ich klientami.
Technologia blockchain jest platformą, którą można wykorzystać na wiele sposobów. Według BIK technologia blockchain optymalizuje i unowocześnia komunikację instytucji z jego klientem. Dodatkowo, co jest bardzo ważne, przechowywanie dokumentów dla klientów na technologii blockchain spełnia wymogi prawne trwałego nośnika informacji. W uproszczeniu, blockchain to rodzaj bazy danych, która zamiast przechowywać dane w centralnym miejscu, przechowuje je w systemie rozproszonym. W formie kolejnych bloków rejestrowane są wszystkie zdarzenia oraz obiekty, każdy z nich zawiera odnośnik kryptograficzny do bloku poprzedzającego. Dodatkowo, dzięki rozproszeniu dokumentów do wielu miejsc przechowywania (uczestników sieci), rozwiązanie gwarantuje integralność i niezaprzeczalność zapisanych informacji. Usunięcie któregokolwiek bloku nie pozostanie bez śladu w systemie. Realizacja trwałego nośnika informacji z wykorzystaniem technologii rozproszonej księgi głównej systemu Billon pozwala spełnić kluczowe jego wymagania: zapewnienie integralności i niezmienności dokumentów przechowywanych w rozproszonej księdze głównej, zapewnienie ciągłości dostępu klienta do jego dokumentów, zapewnienie poufności dokumentów przekazywanych przez instytucję, zapewnienie pełnej ścieżki audytowej wszystkich wykonywanych operacji.
Zaletą zastosowania rozwiązania BIK opartego o blockchain jest wyeliminowanie dokumentów papierowych, których tak bardzo nie lubimy, a przede wszystkim gwarancja niezmienności dokumentów przekazanych klientowi przez dowolną instytucję korzystającą z tego rozwiązania. Dodatkowo, dla osób prywatnych korzyścią będzie posiadanie dostępu do wszystkich dokumentów opublikowanych w ramach rozwiązania w jednym, zaufanym miejscu, na portalu bik.pl. Dzięki takiemu ułatwieniu osoby prywatne będą mogły docelowo zrezygnować z przechowywania dokumentów papierowych, których odszukanie, szczególnie w perspektywie dłuższego czasu bywa bardzo kłopotliwe. W zamian otrzymają proste narzędzie pozwalające na wyszukiwanie dokumentów, np. po instytucji która przekazała, po kategorii dokumentu, po dacie otrzymania. Klient będzie miał łatwy dostęp do swoich dokumentów nawet po ustaniu jego relacji z bankiem, czy inną instytucją.
Jeszcze w tym roku BIK zaplanował wdrożenie swojego rozwiązania blockchain w pierwszych instytucjach, nie tylko finansowych. W pierwszej kolejności będzie to funkcjonalność przechowywania dokumentów, w kolejnych etapach możliwe będzie zdalne podpisywanie umów i aktywne doręczanie dokumentów z potwierdzeniem.

BIK – Cyfrowa Inteligencja

Bartosz Wójcicki dyrektor Biura Usług Antyfraudowych, BIK

Od ponad 20 lat misją BIK jest zapewnienie bezpieczeństwa uczestnikom obrotu gospodarczego w Polsce. Budując konsekwentnie długofalową strategię antyfraudową oraz realizując cel ograniczania ryzyka operacji finansowych na rynku kredytowym i pożyczkowym, BIK wdrożył w 2017 r. Platformę Antyfraudową Cyber Fraud Detection.
Jest to kompleksowe narzędzie, zapewniające efektywną ochronę komunikacji dokonywanej przez klientów instytucji finansowych w kanałach on-line. System obejmuje zarówno obszar sprzedaży produktów oferowanych przez te instytucje, jak rownież proces logowania do aplikacji internetowych i mobilnych czy transakcji zlecanych w kanałach online. Platforma CFD wprowadza możliwość dodatkowej identyfikacji urządzenia, z którego następuje kontakt klienta w kanale online (np. telefon, tablet lub komputer) oraz dokonuje oceny poziomu ryzyka związanego z tym urządzeniem, wykluczając możliwość przeprowadzenia potencjalnego nadużycia w cyfrowym kanale. System pozwala na wykrycie niepożądanej sytuacji, w której przestępca wszedł w posiadanie poprawnego loginu i hasła użytkownika systemu i próbuje dokonać transakcji oszukańczej.
Platforma Cyber Fraud Detection to kolejne rozwiązanie po Platformie Antyfraudowej, które podwyższa stabilność i bezpieczeństwo sektora finansowego w Polsce oraz uwzględnia potrzeby instytucji finansowych w zakresie minimalizacji nadużyć, a tym samym ograniczenia ryzyka operacyjnego.

TEKST PROMOCYJNY

BEZPIECZNY BANK

Kto gwarantuje bezpieczeństwo naszym płatnościom?

Według badania „Płatności cyfrowe 2017"[1] przeprowadzonego na zlecenie Izby Gospodarki Elektronicznej Polacy dokonali znacznego postępu w zakresie korzystania z elektronicznych usług finansowych i transakcyjnych. W październiku 2017 roku aż 45 proc. osób posiadało konto bankowe z aktywnym dostępem przez internet, a 29 proc. korzystało z aplikacji płatniczych na urządzeniach mobilnych.

Leszek **Tasiemski**

wiceprezes ds. badań i rozwoju w firmie F-Secure

Bankowość internetowa sprawiła, że transakcje są wygodniejsze i szybciej realizowane. Użytkownicy oszczędzają czas, a banki pieniądze, ponieważ nakłady na obsługę są mniejsze. Zazwyczaj jednak gdy coś staje się prostsze, cierpi na tym bezpieczeństwo. Klienci są bardzo zróżnicowani pod względem umiejętności obsługi bankowości oraz świadomości zagrożeń. Tym samym użytkownicy, którzy są mniej wyczuleni na zagrożenia, stają się bardziej podatni na cyberataki.

Na przestrzeni ostatnich lat zagrożenia mobilne stały się bardziej powszechne z uwagi na wzrost liczby samych urządzeń. Przykładowo liczba smartfonów na świecie w 2014 roku wynosiła około 1,5 miliarda, a obecnie jest to już 2,5 miliarda. Istnieją pewne zagrożenia, na które warto zwrócić szczególną uwagę podczas korzystania z usług banku na urządzeniu mobilnym.

Spreparowana sieć Wi-Fi

Jedną z metod stosowaną przez hakerów jest próba przejęcia danych logowania do banku przy pomocy spreparowanej sieci Wi-Fi. Podatna na tego typu cyberataki są osoby, które logują się do publicznie dostępnych punktów sieciowych (tzw. hotspotów). Cyberprzestępca może z łatwością zabrać swój własny router do galerii handlowej i stworzyć sieć Wi-Fi, którą dla niepoznaki nazwie tak samo jak nazywa się sieć restauracji, w której akurat będzie przebywać potencjalna ofiara. W dodatku haker może przyciągać ogólną dostępnością i brakiem konieczności wpisywania loginu i hasła. Po połączeniu z taką siecią, a następnie skorzystaniu z usług bankowych (w szczególności z poziomu przeglądarki internetowej zamiast dedykowanej aplikacji), haker mógłby podejrzeć, jakie dane logowania do banku zostały wprowadzone przez użytkownika.

Przestarzały system operacyjny

Cyberprzestępcy mogą również wykorzystać luki w starych wersjach systemu, aby przejąć kontrolę nad słabo zabezpieczonym urządzeniem, co stanowi kolejne zagrożenie dla sesji bankowych. W szczególności dotyczy to popularnego Androida, który jest stosowany przez 85 proc. użytkowników w skali globalnej[2]. Według danych z 7 maja 2018 roku z najnowszej wersji Androida Oreo korzysta niecałe 6 proc. użytkowników[3], a z poprzedniej – Nougat, około 31 proc. Niemieckie laboratorium antywirusowe AV-TEST na przestrzeni trzech lat zanotowało ponad 15 milionów próbek złośliwego oprogramowania na system Android[4].

Nieoficjalna aplikacja bankowa

Cyberprzestępcy wykorzystują również niski poziom autoryzacji aplikacji w sklepie Google'a oraz możliwość instalacji oprogramowania z niezaufanych źródeł. W październiku 2017 roku polskie instytucje finansowe przestrzegały przed aplikacją do śledzenia kursu kryptowalut, która była dostępna do pobrania z autoryzowanego sklepu. Po jej zainstalowaniu wyświetlała się specjalna nakładka udająca oficjalną aplikację bankową, w której użytkownicy byli proszeni o wpisanie swoich danych logowania. Tym samym cyberprzestępcy otrzymywali dostęp do konta. Wirus przejmował również kontrolę nad telefonem i dawał możliwość podsłuchiwania połączeń telefonicznych, a także wysyłania i odczytywania treści SMS-ów (w tym wiadomości potwierdzających transakcję z bankiem).

Wzmożone ataki typu phishing

Phishing to podszywanie się pod osobę lub instytucję w celu wyłudzenia danych i jest to wciąż jedna z najbardziej skutecznych metod stosowana przez cyberprzestępców. Dlatego należy podchodzić ze szczególną ostrożnością do e-maili pochodzących z nieznanych źródeł (lub podszywających się pod komunikację z bankiem) i w takich przypadkach nie klikać w załączniki. To samo dotyczy sms-ów oraz linków przesyłanych przez komunikatory.

Jak się chronić?

Podstawowym środkiem bezpieczeństwa jest stosowanie skomplikowanych haseł – innych do każdego z odwiedzanych serwisów. Należy unikać stosowania tego samego hasła w kilku serwisach, ponieważ rośnie ryzyko utraty wielu kont jednocześnie – dotyczy to szczególnie bankowości internetowej. Równie niebezpieczne byłoby korzystanie z jednego klucza do zamku w domu, samochodzie oraz sejfie. Zalecane jest stosowanie możliwie długiego i skomplikowanego hasła. Trudne do złamania hasło to kombinacja kilkunastu różnych znaków – wielkich i małych liter, cyfr, symboli czy spacji.

Warto pamiętać, że cyberprzestępca może próbować odgadnąć hasło do profilu, który go interesuje, na podstawie poprzednio wykorzystywanych haseł danego użytkownika. Istnieją jednak strony internetowe takie jak https://haveibeenpwned.com/, które umożliwiają sprawdzenie czy konta zostały zhakowane. Jeżeli do tego doszło, należy jak najszybciej zmienić dane logowania. Warto rozważyć korzystanie z menadżera haseł, który pomaga generować unikalne klucze przechowywane w jednym miejscu.

Użytkownicy urządzeń mobilnych często zakładają, że oprogramowanie antywirusowe jest niezbędne wyłącznie na komputerze. Aby zadbać o bezpieczeństwo, warto zainstalować na urządzeniu mobilnym oprogramowanie ochronne, które nie tylko strzeże przed wirusami, ale blokuje szkodliwe strony internetowe czy uniemożliwia nawiązanie połączenia z innymi witrynami w czasie transakcji bankowych.

Ze względu na izolację aplikacji na platformach mobilnych są one bardziej bezpieczne niż tradycyjne systemy operacyjne z aplikacjami przeglądarkowymi. W przypadku platform mobilnych za każdą czynność najczęściej odpowiada inna aplikacja – np. bankowa, związana z konkretnym portalem społecznościowym czy aukcyjnym. Przepływ danych między tymi aplikacjami jest z reguły całkowicie zablokowany albo przynajmniej znacząco ograniczony, co również ma wpływ na bezpieczeństwo.

Warto upewnić się jednak, czy strona internetowa banku prowadzi do tej samej aplikacji, którą mamy zamiar pobrać ze sklepu oraz spojrzeć na opinie użytkowników i pamiętać, że należy zaprzestać logowania się i zgłosić problem do banku, jeżeli tylko coś wyda nam się podejrzane. Kluczowe jest także przeprowadzanie regularnych aktualizacji – zarówno poszczególnych aplikacji, jak i systemu wykorzystywanego przez urządzenie mobilne.

1. http://eizba.pl/files/9315/1125/8342/platnosci_cyfrowe_20172.pdf

2. https://www.statista.com/topics/876/android/

3. https://developer.android.com/about/dashboards/index.html

4. Od stycznia 2013 roku do sierpnia 2016

Deszcz monet z chmury

Instytucje finansowe stoją przed koniecznością ciągłego rozwijania źródeł przychodów. By przetrwać, poza poprawą doświadczeń klientów w nowych kanałach komunikacji, są one zmuszone do nieustannego poszukiwania oraz kreowania nowych produktów finansowych i usług.

Andrzej **Gibas**

dyrektor sprzedaży do sektora Financial Services w polskim oddziale Microsoft

Konieczność błyskawicznego rozwoju aplikacji biznesowych wzmaga zainteresowanie menedżerów możliwościami chmury obliczeniowej. Wielu decydentów w instytucjach bankowych jest przekonanych o korzyściach płynących z przeniesienia wybranych procesów do chmury, ale przed jej finalnym wyborem wciąż mają szereg wątpliwości, co w opinii bankowców wynika z niejasnego stanowiska polskiego regulatora wobec chmury.

Cała nadzieja w cloud

Najnowszy komunikat UKNF z 24 października 2017 roku dotyczący korzystania przez podmioty nadzorowane z usług przetwarzania danych w chmurze obliczeniowej, świadczy o pozytywnym podejściu regulatora sektora bankowego do wdrażania w bankach nowoczesnych rozwiązań informatycznych w postaci chmury obliczeniowej zarówno publicznej, jak i w modelu hybrydowym. Dzięki możliwościom oferowanym przez chmurę, banki mogą poprawić sprawność dostarczania aplikacji bankowych, proponując tradycyjne usługi na nowych rynkach, nawet wchodząc w partnerstwa z FinTechami. Świetnym przykładem realizacji takiej polityki jest Bank Millennium, który dzięki usługom chmurowym rozwinął platformę goodie łączącą bank, klientów i detalistów w ramach platformy e-commerce, sprzedającej ofertę produktów i usług online.

Rewolucja sztucznej inteligencji

Dane to siła napędowa cyfryzacji, których zasoby lawinowo przyrastają w każdej organizacji. By stały się faktycznym paliwem wzrostu i zapewniły nowe źródła przychodów wymagają zastosowania odpowiednich narzędzi z obszaru analityki, machine learning i sztucznej inteligencji (AI). To właśnie dzięki AI, instytucje finansowe mają szansę wprowadzić szereg innowacji dotyczących doświadczeń klientów w dowolnym kanale komunikacji i wielu obszarach swojej działalności, takich jak obsługa klienta, koszty, efektywność operacyjna, wykrywanie nadużyć, lepsza ocena ryzyka, bezpieczeństwo czy podejmowanie decyzji. Sztuczna inteligencja może zautomatyzować zadania realizowane manualnie, takie jak generowanie raportów lub odpowiadanie na typowe zapytania, zautomatyzować żmudne i powtarzalne procesy pracy, dając czas pracownikom na realizację zadań o większej wartości dodanej. AI ma także potencjał do przekształcania całych modeli biznesowych i rewolucjonizuje bardziej strategiczne funkcje, takie jak analiza finansowa, alokacja aktywów i prognozowanie.

Monetyzacja danych jest nierozerwalnie związana z rozwojem sztucznej inteligencji. Już teraz szybko transformujące się instytucje finansowe, które najsprawniej zarządzają danymi i są w stanie przekształcić je na wymierny zysk, znajdą się na drodze do poprawy efektywności operacyjnej i lepszego dotarcia do klientów.

Podpisano porozumienie ze Związkiem Banków Polskich

Centrum Elektronicznych Usług Płatniczych – eService, Związek Banków Polskich i Warszawski Instytut Bankowości podpisały porozumienie w sprawie dołączenia do programu „Bezpieczeństwo w Cyberprzestrzeni". W ramach inicjatywy będą prowadzone działania edukacyjne na rzecz popularyzacji i bezpiecznego funkcjonowania obrotu bezgotówkowego. – Cyberbezpieczeństwo jest jednym z tych obszarów, w których należy współpracować, a nie konkurować. Wierzę, że połączenie naszych praktyk i doświadczeń oraz specjalistycznej wiedzy skumulowanej w firmach infrastrukturalnych sektora bankowego i technologicznego będzie podstawą powodzenia naszej misji edukacyjnej. Chcemy prowadzić ja za pomocą zróżnicowanych działań i form, by dotrzeć do jak największej liczby odbiorców – w tym dzieci, młodzieży, studentów i seniorów. Tego typu wiedza jest we współczesnym świecie niezbędna dla każdego, kto posługuje się kartą płatniczą, komputerem czy telefonem – ocenia Krzysztof Pietraszkiewicz, prezes Związku Banków Polskich.

Dostawcy usług cyfrowych pod nadzorem krajowego systemu cyberbezpieczeństwa

Polski rząd przyjął niedawno ustawę o krajowym systemie cyberbezpieczeństwa wypełniającą założenia europejskiej Dyrektywy NIS, dotyczącej bezpieczeństwa sieci i informacji. Głównym założeniem nowych przepisów ma być zapewnienie ochrony cyberprzestrzeni na poziomie krajowym. Ustawa obejmie swoim zasięgiem przede wszystkim dostawców usług cyfrowych, którzy będą musieli szybko raportować każdy incydent związany z cyberbezpieczeństwem. W myśl nowych przepisów NIS (Network and Information Security Directive) m.in. internetowe platformy handlowe, usługodawcy oferujący przetwarzanie w chmurze i dostawcy wyszukiwarek internetowych będą musieli spełnić szereg wymogów związanych z ochroną danych i raportowaniem incydentów zagrażających bezpieczeństwu. – Raportowanie incydentów dla firm sektora energetycznego, transportowego, bankowości, dostawców usług cyfrowych i całego sektora publicznego będzie oznaczało, że firmy te będą musiały mieć odpowiednie osoby, procedury i narzędzia, które pozwolą na to, żeby wykrywać incydenty bezpieczeństwa, a potem klasyfikować je i w bardzo krótkim czasie, bo w ciągu 24 godzin, przedstawić raport na temat krytycznego, poważnego czy istotnego incydentu bezpieczeństwa – wyjaśnia w rozmowie z agencją informacyjną Newseria Innowacje Mariusz Stawowski z firmy Clico dostarczającej produkty zapewniające bezpieczeństwo danych.

Potrzeba strategicznego myślenia

Przedsiębiorcy, bardziej niż jakakolwiek inna grupa zawodowa, powinni być świadomi tego, że wkraczamy w erę cyfrowej rewolucji, w której informacje stały się nową walutą. Jesteśmy coraz bardziej zależni od bezpieczeństwa naszych danych. Mimo to, według badania „Cyber Threat CEE Region 2018" przeprowadzonego przez platformę CYBERSEC HUB wśród przedstawicieli MŚP z Europy Środkowo-Wschodniej, aż 65 proc. firm z regionu, a 47 proc. w Polsce, nie ma opracowanej strategii cyberbezpieczeństwa, tylko połowa z nich tworzy regularnie kopie danych, a niemal 60 proc. wciąż stawia przede wszystkim na klasyczne oprogramowanie antywirusowe. – Trudno oszacować starty światowego biznesu ponoszone z powodu cyberataków, ale powszechnie uważa się, że wynoszą od 1 do 3 proc. globalnego PKB. Skala tego zjawiska wyraźnie wskazuje, że nasza gospodarka jest w dużym stopniu zależna od bezpieczeństwa infrastruktury teleinformatycznej, a cyberbezpieczeństwo musi być nieodłącznym elementem nadchodzącej czwartej rewolucji przemysłowej" – komentuje Robert Siudak, CYBERSEC HUB Manager.

SECURITY AWARENESS – edukacja i kultura bezpieczeństwa w każdej organizacji

Dobrze zarządzaną organizację cechuje pewien wyróżnik, a mianowicie zaangażowanie pracowników w jej funkcjonowanie. Oprócz procesów, produktów, planów podstawową wartością każdego przedsiębiorstwa są ludzie. To od ich wiedzy, motywacji i zaangażowania zależy sukces rynkowy firmy. Nie inaczej wygląda to od strony bezpieczeństwa. W dobie tak licznych zagrożeń związanych z cyberprzestępczością nawet najdoskonalsze systemy techniczne nie są w stanie, bez współudziału człowieka, uchronić nas przed atakiem. W związku z tym odpowiedzialność za cyber bezpieczeństwo powinna spoczywać na każdej osobie zatrudnionej w przedsiębiorstwie, a nie tylko na barkach zarządu. Uświadamianie jednak pracowników to najtrudniejsze, ale jednocześnie najważniejsze zadanie dla osób odpowiedzialnych za bezpieczeństwo w firmie.

W idealnym systemie każdy pracownik powinien mieć poczucie, że uczestniczy w procesach odpowiadających za bezpieczeństwo cybernetyczne firmy. Poprzez edukację można wyeliminować nawet do 90 procent wszystkich zdarzeń związanych z bezpieczeństwem informatycznym.
Edukacja, oprócz podwyższenia świadomości pomaga także w implementacji rozwiązań do ochrony chociażby takich jak system klasyfikacji informacji.
Systemy do klasyfikacji informacji pozytywnie wpływają na zwiększenie świadomości pracowników i współpracowników organizacji w zakresie ochrony danych oraz ich przetwarzania, tworząc stabilny pomost łączący człowieka z rozwiązaniami technicznymi.
Rozwiązania bezpieczeństwa zintegrowane z systemem klasyfikacji informacji, umożliwiają – w czasie rzeczywistym – interpretację oraz odczyt zarówno kontekstu, jak i atrybutów dokumentów, takich jak: lokalizacja, typ pliku, czy jego twórca. Integracja ta zapewnia precyzyjne określenie wagi przetwarzanych informacji oraz zastosowanie procedur ochrony w odniesieniu do plików i poczty elektronicznej.

Dlaczego warto wykorzystywać ręczne systemy do klasyfikacji?
Rozwiązania do klasyfikacji wprowadzają możliwość uzupełnienia mechanizmów automatycznie kategoryzujących dokumenty oraz pocztę elektroniczną, o nieocenioną w takich przypadkach wiedzę użytkownika o wadze przetwarzanych przez niego danych.
Codzienne obcowanie z kategoriami dokumentów oraz odręczne klasyfikowanie dokumentów czy poczty elektronicznej podnosi świadomość pracowników, dotyczącą zagadnień bezpieczeństwa oraz ważności przetwarzanych przez nich informacji. Kategoria każdego dokumentu zależy od przemyślanej decyzji autora lub osoby przetwarzającej dany dokument – mającej świadomość wagi zawartej w nim informacji. Możliwość oznaczania dokumentu istnieje zarówno podczas jego tworzenia, edytowania, przeglądania lub rozpowszechniania.

Dlaczego GREENmod?
Jedyne polskie rozwiązanie do klasyfikacji informacji firmy TUKAN IT wymusza konieczność sklasyfikowania tworzonego dokumentu przed jego zapisaniem. Analogicznie, GREENmod uniemożliwi wysłanie wiadomości pocztowej, jeżeli nie zostanie ona sklasyfikowana.
Znaczniki nadawane w procesie klasyfikacji są łatwo rozpoznawane przez różnego rodzaju rozwiązania analizujące treść i właściwości dokumentów (systemy DLP, RMS, rozwiązania mail i web proxy, itp.). Na ich podstawie możliwe jest skuteczne egzekwowanie przyjętej w organizacji polityki bezpieczeństwa i świadome podejmowanie decyzji dotyczących sposobu obsługi, przetwarzania oraz ochrony danych, zapewniając optymalizację kosztów.

> Wykorzystanie rozwiązania Tukan IT GREENmod w organizacji znacząco wpływa na podnoszenie świadomości pracowników, dotyczącej zagadnień bezpieczeństwa oraz ważności przetwarzanych przez nich informacji. W efekcie spada także liczba wycieków informacji, które wynikają z czynności wykonywanych bez zastanowienia lub z braku wiedzy na temat tego, jakie są skutki udostępnienia chronionych treści osobom nieupoważnionym.

Użytkownik przetwarzający dane, ocenia ich wagę dla organizacji i nadaje stopień klasyfikacji, a system przypisuje obiektom ukryty znacznik, zapisywany w metadanych.

GREENmod zapewnia łatwe wdrożenie, elastyczną konfigurację, możliwość tworzenia własnych kategorii i podkategorii klasyfikacji oraz wymuszanie na użytkownikach kategoryzacji obiektów. GREENmod pomaga w podjęciu decyzji nadania klasyfikacji poprzez wykorzystanie systemu wirtualnej pomocy, zarówno w postaci kreatora, okien pomocy, odnośników do udostępnianych przez organizację baz wiedzy oraz filmów instruktażowych.
Łatwy w użyciu i przyjazny interfejs rozwiązania zapewnia szybkość implementacji i akceptację przez użytkowników końcowych, którzy szybko dostrzegą wartość wdrożonego systemu.
Wykorzystanie rozwiązania Tukan IT GREENmod w organizacji znacząco wpływa na podnoszenie świadomości pracowników, dotyczącej zagadnień bezpieczeństwa oraz ważności przetwarzanych przez nich informacji. W efekcie spada także liczba wycieków informacji, które wynikają z czynności wykonywanych bez zastanowienia lub z braku wiedzy na temat tego, jakie są skutki udostępnienia chronionych treści osobom nieupoważnionym. Pracownicy, którzy są zaangażowani w proces zapewniania bezpieczeństwa, stają się bardziej odpowiedzialni za informacje, które tworzą.

Tukan IT GREENmod:
- angażuje użytkowników w proces klasyfikowania informacji,
- umożliwia dostosowanie struktury klasyfikacji do własnych potrzeb,
- integruje się z systemami chroniącymi i przetwarzającymi informacje,
- posiada centralne zarządzanie i raportowanie,

pomaga ustalić odpowiedzialność i właściciela informacji,
- wspomaga procedury audytowe,

obniża koszty zabezpieczania informacji.

TEKST PROMOCYJNY