OPROGRAMOWANIE DLA INSTYTUCJI FINANSOWYCH

W poszukiwaniu źródeł finansowania

Cyfrowa transformacja biznesu, w tym szczególnie firm MŚP stanowiących zwykle główną siłę europejskich gospodarek, jest priorytetem unijnego portfela inwestycji. W puli Programu „Cyfrowa Europa", na lata 2021-2027 do przekazania przedsiębiorcom są środki w wysokości 7,5 mld euro. W minionym roku przyznano z niej europejskim firmom 1,13 mld euro, w tym zaś planowana kwota jest jeszcze większa i wynosi blisko 1,25 mld euro.

Adam **Wojtkowski**
General Manager CEE, Red Hat

A to jedynie podnóże imponującej góry środków dla firm poszukujących wsparcia w obszarze digitalizacji czy transformacji cyfrowej. Ogólnie rzecz biorąc, źródeł finansowania procesów cyfryzacyjnych nie brakuje – pytanie jednak, jak sensownie ulokować te środki, by oczekiwania firm „spotkały" się z efektami oraz by zakupione narzędzia były realne przydatne przez wiele lat?

Kontynentalnie oraz lokalnie

Poza „Cyfrową Europą" UE ma w zanadrzu także takie programy finansowania, jak m.in. Connecting Europe Facility (ponad 2 mld euro), wspierający rozbudowę infrastruktury sieciowej dla sektorów transportu, telekomunikacji oraz energetycznego, czy InvestUE (26,2 mld euro) dedykowany wysiłkom rekonstrukcji biznesu po pandemii, ukierunkowany głównie na cyfryzację oraz zakup nowych technologii.

Jeśli natomiast przedsiębiorcy wolą sięgać po finansowanie za pośrednictwem krajowych instytucji, warto zapoznać się z aktualnymi programami zarządzanymi przez PARP. Dla przykładu, w ramach Bonów na cyfryzację, dostępnych w III kwartale minionego roku, firmy mogły otrzymać nawet 255 tys. zł dofinansowania na zakup oprogramowania, w tym usług chmurowych, jak również sprzętu informatycznego. W drugim kwartale 2022 ruszy natomiast kolejna część wsparcia realizowana z Funduszy Europejskich, dzięki której przedsiębiorcy będą mogli pokryć koszty działalności badawczo-rozwojowej oraz wdrażania innowacji i narzędzi technologicznych. Najszybciej przekazane do wypłat będą środki z pierwszego priorytetu Programu Fundusze Europejskie dla Nowoczesnej Gospodarki (FENG) – wsparcie dla przedsiębiorców, których łączna wartość wyniesie ponad 20 mld zł.

Dobry wniosek to podstawa

Program Fundusze Europejskie dla Nowoczesnej Gospodarki, z budżetem ok. 7,9 mld euro, wystartuje w drugiej połowie roku, stąd też szczegóły dotyczące samej procedury wzięcia udziału w naborze wniosków nie są jeszcze znane. Wiadomo, że duże firmy, a także konsorcja MŚP z korporacjami i organizacjami badawczymi będą obsługiwane przez Narodowe Centrum Badań i Rozwoju, małe i średnie przedsiębiorstwa zaś przez PARP. Jak w praktyce wygląda wzięcie udziału w podobnym konkursie, można jednak zaobserwować na przykładzie zakończonego w październiku minionego roku programu „Bony na Cyfryzację". Ten adresowany był wyłącznie do mikro, małych oraz średnich przedsiębiorstw działających na terenie Polski. Wniosek pobierany ze strony programu w serwisie PARP liczył 15 stron i choć na pierwszy rzut oka mógł wydawać się skomplikowany, opatrzony był także szczegółową instrukcją wypełniania. Ponadto dedykowany inicjatywnie portal www.bonynacyfryzacje.pl umożliwiał także zlecenie przygotowania wniosku jako kompleksową pomoc adresowaną w szczególności do przedsiębiorców pierwszy raz zwracających się o dofinansowanie ze środków europejskich. Wnioskujący mogli otrzymać do 255 tys. zł bezzwrotnej dotacji, pod warunkiem że zgromadzili 15 proc. wkładu własnego dla ogółu kosztu projektu. Rozstrzygnięcie konkursu trwało natomiast 100 dni od momentu zamknięcia naboru wniosków.

Po co mi w ogóle zmiana?

Tylko w 2021 r., w ramach 3 programów wsparcia (POIR, POPW, POWER) złożono ponad 13 tys. wniosków. Wysokie zainteresowanie sięganiem po dofinansowania z funduszy europejskich wynika w dużej mierze z potrzeby coraz częstszego sięgania po cyfrowe produkty pozwalające utrzymać, a także zwiększać konkurencyjność rynkową. Digitalizacja jest dzisiaj niezbędna w niemal każdym obszarze zarządzania firmą – od interakcji z klientami, którzy oczekują łatwiej-

szych, intuicyjnych i spersonalizowanych metod cyfrowego kontaktu, przez administrację finansowo-księgową, po narzędzia automatyzujące analizę danych z wielu źródeł i dostarczające wnioski istotne z biznesowego punktu widzenia. Ważną rolę odgrywa także proces przechodzenia od posiadania sprzętu IT oraz aplikacji on-premise, czyli „na pokładzie" firmy do zakupu usług chmurowych, znoszących konieczność inwestowania w sprzęt, oprogramowanie, a nawet wyspecjalizowany personel zarządzający infrastrukturą na rzecz subskrypcji.

Niewątpliwą zaletą przejścia na drogę cyfrowej transformacji jest również wzrost przewagi konkurencyjnej. Konsumenci – także ci z sektora B2 B – przyzwyczaili się do prostych, wygodnych i zautomatyzowanych rozwiązań, których nie da się zapewnić bez nowoczesnej infrastruktury IT i odpowiedniego zaplecza technologicznego rozumianego także jako oprogramowanie, które jest w stanie sprostać nieustannie zmieniającym się potrzebom i oczekiwaniom rynku. To jak ważna jest cyfrowa transformacja, pokazały ostatnie dwa lata walki z pandemią. Firmy, które wcześniej zainwestowały w rozwój swoich działów IT, znacznie łagodniej przeszły kryzys i były w stanie niemal z dnia na dzień przenieść się na pełni cyfrowy świat pracy, obsługi swoich klientów, sprzedaży czy serwisu. Przestarzałe rozwiązania, szczególnie te z zakresu zastrzeżonego oprogramowania okazały się zbyt trudne do zmiany, a w wielu przypadkach zmiana nie była w ogóle możliwa.

Kiedy rozmawiamy z naszymi klientami, to obok wielu zalet cyfrowej transformacji związanych choćby z łatwością zarządzania swoją infrastrukturą IT, dostarczaniem nowych rozwiązań czy aplikacji, to zawsze słyszymy, że przejście na OpenSource znakomicie wpłynęło na ich efektywność kosztową oraz uproszczenie wielu procesów. Tego typu rozwiązania pozwalają bowiem na niemal ekspresowe dopasowywanie się do potrzeb każdego użytkownika, a jednocześnie są znacznie prostsze w obsłudze.

Kierunkowskazy cyfryzacji

Jest zatem o co się starać. Jednak pozyskanie finansowania przeznaczonego na unowocześnienie zarządzania firmą przez nowe technologie to zaledwie pierwsza część strategii. Druga, równie istotna to opracowanie planu ich wydatkowania na rozwiązania, które nie tylko odciążą personel czy otworzą nowe możliwości biznesowe, ale także nie będą generować zbyt dużych kosztów w dłuższej perspektywie czasu.

Jak pokazują nasze doświadczenia, firmy w gąszczu dostępnych rozwiązań i systemów do cyfryzacji poszczególnych obszarów przedsiębiorstwa często nie wiedzą jakiego typu rozwiązania wybrać i jak dalece będą one dla nich efektywne w przyszłości. Pamiętajmy, że są to zwykle dość spore inwestycje, i choć realizowane przy wsparciu funduszy, należy o nich myśleć długofalowo. Wybór „zamkniętych" systemów oznacza, że ich możliwości w zakresie przyszłej rozbudowy wraz z rozwojem firmy czy połączenia z nowymi narzędziami są ograniczone. Stawiając na usługi otwarte, typu open-source, gwarantują sobie jednocześnie dowolność w zakresie ich modyfikacji, łączenia z wieloma chmurami od różnych dostawców czy skalowania w zależności od potrzeb.

Dziś, z racji na dynamiczne zmiany na rynkach, adaptację zaawansowanych rozwiązań takich jak sztuczna inteligencja, analityka Big Data czy blockchain oraz niemal nieustanną potrzebę przygotowywania środowisk IT na kolejne, nowe wyzwania, dominującym trendem staje się sięganie po technologie open-source. Są to produkty cyfrowe z tzw. otwartym kodem, a więc te, które pozwalają niemal dowolnie się konfigurować i adaptować do wszelkich zmian, jakie następują w cyfrowym środowisku firmy. Jak wynika z badania Red Hat – The State of Enterprise Open Source, dziś już 90 proc. liderów IT w organizacjach z całego świata stosuje oprogramowanie open-source. Ośmiu na dziesięciu jest przekonanych, że tego typu narzędzia pozwolą im wdrożyć najnowsze i najbardziej złożone technologie w firmach, 87 proc. uważa zaś aplikacje open-source za tak samo lub nawet bardziej bezpieczne niż klasyczne, „zamknięte". Warto wspomnieć, że największe instytucje i światowe korporacje – w tym banki – korzystają z dobrodziejstw takich technologii jak OpenShift czy Kubernetes, dzięki czemu spadają ich wydatki, a czas opracowywania nowych rozwiązań informatycznych zostaje wyraźnie skrócony.

OpenSource nierówny OpenSource – dlaczego warto wybrać płatne i pewne rozwiązania

Oprogramowanie open source jest tworzone w sposób zdecentralizowany, oparty na współpracy społeczności programistów z całego świata. Szacuje się, że obecnie na świecie istnieje ponad 18 mln projektów o otwartym kodzie źródłowym. To ogromna kopalnia potencjalnych innowacji w takich dziedzinach jak sieć 5G, chmura hybrydowa czy sztuczna inteligencja i uczenie maszynowe.

W przeciwieństwie do licencji na oprogramowanie zamknięte, subskrypcje open source dotyczą całego cyklu życia produktu, w ramach którego będą dostarczane ulepszenia, poprawki błędów i łatki bezpieczeństwa. Warto zaznaczyć, że klienci mają prawo do nieograniczonych aktualizacji w ramach trwającej subskrypcji, ale nigdy nie są do nich zmuszani – to klient decyduje, która wersja np. systemu operacyjnego zapewnia największą stabilność jego usługi biznesowej.

Co więcej, subskrypcje oprogramowania open source zapewniają gotowe, certyfikowane i przede wszystkim bezpieczne rozwiązania dla przedsiębiorstw. Posiadając subskrypcję, mamy pewność, że nad oprogramowaniem czuwa zespół programistów (często wywodzących się ze społeczności open source), którzy codziennie analizują zagrożenia i luki w zabezpieczeniach, opracowują poprawki, jak również służą pomocą, gdy użytkownik potrzebuje wsparcia technicznego. Nabywca subskrypcji może zatem spać spokojnie, ponieważ ma pewność, że dostawca zareaguje i bezzwłocznie wdroży odpowiednie aktualizacje.

Open-source „urośnie" podwójnie, a Twoja firma razem z nim

O tym, że oprogramowanie z kodem otwartym ma szansę być rozwiązaniem pierwszego wyboru informuje również analiza MarketsAndMarkets, na którą powołuje się słynny serwis VentureBeat. Zgodnie z nią, rynek produktów tego typu ma z poziomu 21,7 mld $ na koniec minionego roku wzrosnąć ponad dwukrotnie, do wartości 50 mld $ w ciągu pięciu najbliższych lat.

Biorąc pod uwagę wszystkie te aspekty, warto się pochylić nad przygotowaniem dobrego wniosku i pozyskać europejskie lub krajowe finansowanie cyfrowej drogi swojej firmy. Mądrze dobrane rozwiązania sprawią, że każdy przedsiębiorca zyska nowe możliwości rozwoju i będzie znacznie lepiej zabezpieczony na wypadek kolejnych zdarzeń takich jak towarzysząca nam obecnie pandemia.

Szanowni Państwo
Czy instytucje finansowe potrzebują innego oprogramowania niż przedsiębiorstwa reprezentujące inne branże? Z pewnością tak. A czy firmy projektujące oprogramowanie mają świadomość szczególnych potrzeb banków, ubezpieczycieli, firm leasingowych i innych przedstawicieli rynku finansowego? Patrząc na to, jak przygotowują dla nich swoją ofertę, zapewne tak. Zapraszamy Państwa do analizy zaprezentowanych przez „Gazetę Finansową" ofert przygotowanych właśnie z myślą o instytucjach finansowych – zobaczcie, co dziś jest istotne z punktu widzenia tego sektora i na co może liczyć.

Redakcja

NAJLEPSZE OPROGRAMOWANIE DLA INSTYTUCJI FINANSOWYCH

Nazwa firmy	Nazwa programu dla instytucji finansowej	Opis programu
Asseco Data Systems	LEO System® 4.0	LEO System® 4.0 służy do kompleksowego zarządzania produktami i kontraktami leasingowymi. To intuicyjne w obsłudze oprogramowanie jest przeznaczone dla firm leasingowych bez względu na ich wielkość, profil czy portfolio. Wspiera zarządzanie zarówno prostymi transakcjami o dużym wolumenie, jak i złożonymi, strukturyzowanymi kontraktami leasingowymi w dowolnej walucie. Rozwiązanie umożliwia projektowanie i automatyzację procesów biznesowych w myśl zasady, że to praca szuka człowieka a nie człowiek pracy. Jednocześnie dzięki zastosowaniu API ułatwia integrację z innymi systemami pozwalając wpisać się w dowolną architekturę systemów. Zaawansowane funkcje zapewniają kompleksową obsługę życia kontraktów leasingowych wraz z produktami dodatkowymi jak różnego rodzaju ubezpieczenia, usługi CFM (karty paliwowe, opony, przeglądy). Zintegrowana część finansowo-księgowa zapewnia realizację operacji księgowych oraz przygotowanie raportów. LEO System® 4.0 jest dostępny w modelu on premise oraz SaaS.
Asseco Poland	Wspólna Platforma Informatyczna (WPI)	WPI to dla banku spółdzielczego eliminacja inwestycji i przewidywalność kosztów. Platforma jest dostępna w modelu chmurowym, co zmniejsza koszty związane z posiadaniem odrębnej infrastruktury i zasobów do ich utrzymania. Asseco przejmuje odpowiedzialność za infrastrukturę sprzętową, utrzymanie serwerowni, licencje i aktualizacje oprogramowania, a także takie czynności jak zamknięcia dnia/miesiąca/roku. W ramach jednej opłaty abonamentowej banki spółdzielcze otrzymują wszystko, co jest niezbędne do bieżącego funkcjonowania oraz rozwoju współczesnej instytucji finansowej. Nowa oferta banków może być więc wdrażana szybciej, a wspólne procesy księgowe, sprzedażowe, czy informacji zarządczej, pozwalają na obniżenie kosztów i nie ograniczają autonomii banków m.in. w zakresie parametrów handlowych, wysokości oprocentowania czy pobieranych opłat i prowizji.
Comarch	Comarch EDI	Ponad dwudziestoletnie doświadczenie w masowej komunikacji EDI pomiędzy partnerami B2 B, B2G oferowane klientom platformy Comarch EDI wchodzi na nowe obszary. Tak popularna usługa w modelu SaaS (Software as a Service) niewymagająca dużych nakładów początkowych jest z powodzeniem użytkowana przez tysiące klientów tej platformy. Od kilku lat firma podłącza swoich klientów do platform rządowych w modelu clearance tak, by mogli wysyłać e-faktury zgodnie z prawem poszczególnych krajów. W ostatnich latach wykonała integrację z rozwiązaniami w Niemczech i Polsce – PeF (B2G), Włoszech czy Turcji, a w ostatnich tygodniach uruchomiła podobne rozwiązanie w Rumunii. W 2022 r. nadszedł czas na wykorzystanie sprawdzonej technologii na rynku polskim. Comarch EDI oferuje obecnym, ale także nowym klientom podłączenie ich systemów fakturujących w oparciu o technologię EDI do KSeF już obecnie. Podłączenie nie wymaga dużych nakładów po stronie klienta. Wystarczy zdolność jego systemu ERP/FK do wygenerowania/przyjęcia pliku strukturalnego zawierającego wymagane prawem dane z faktury i połączenie się z Comarch EDI szyfrowanym połączeniem. O resztę zadba firma, tzn. skonfiguruje narzędzia umożliwiające autoryzację podatnika tokenem i wystawienie lub odbiór pliku zgodnego ze schematem KSeF XML. Wykona konwersję plików (mapowanie do/z formatu klienta do wymaganego przez KSeF). Przed wysłaniem do KSeF zwaliduje poprawność przygotowanej przez klienta faktury. Będzie całodobowo monitorować komunikację z KSeF, odbierać statusy zwrotne w tym UPO, i przekazywać je podatnikom. Udostępnia również swoim klientom narzędzia monitorujące transmisję do i z KSeF, śledzenie jej poprawności, raportowanie ewentualnych błędów. To wszystko w atrakcyjnej opłacie abonamentowej. Również inne, dodatkowe usługi na tym polu, jak generowanie faktur dla odbiorców zagranicznych, routowanie dokumentów po zadanych parametrach do wskazanych systemów odbiorczych będą obsługiwane w ramach rozbudowywanej funkcjonalności platformy Comarch EDI dla KseF.
Comarch	Comarch Open Platform	Comarch Open Platform to zaawansowane rozwiązanie technologiczne stworzone dla instytucji finansowych, umożliwiające budowanie najwyższej jakości ekosystemów produktów i usług usprawniających obsługę klientów biznesowych poprzez kanały cyfrowe. Platforma oferuje zestaw zintegrowanych i sprawdzonych narzędzi oraz gotowych modułów produktowych wykorzystywanych do budowania pełnych i zautomatyzowanych procesów z obszaru bankowości transakcyjnej, kredytów, finansowania handlu, faktoringu i wielu innych. Otwarta rozproszona architektura oparta o mikroserwisy i mikrofrotendy w połączeniu ze sprawdzonymi narzędziami technicznymi pozwala na równoległy niezależny rozwój środowiska i szybkie systematyczne dostarczanie wartości Klientom końcowym. Zawarte procesy devOps optymalizują ciągły rozwój i integracje. Zestaw gotowych modułów produktowych pozwala na szybkie zbudowanie i dostarczenie wartości Klientom, a ich otwarty charakter zezwala na dalszy rozwój w ramach własnych zasobów IT, z Comarch bądź zewnętrznym dostawcą usług IT.
DomData AG	Ferryt Low-Code Development	Ferryt Low-Code Platform to kompletne narzędzie dedykowane do szybkiego tworzenia rozwiązań biznesowych i kompleksowego zarządzania procesami biznesowymi w instytucjach finansowych i innych organizacjach. Pozwala na modelowanie procesów, projektowanie ekranów, tworzenie szablonów dokumentów, zarządzanie danymi, integrację z innymi systemami oraz na monitorowanie i analizę wdrażanych rozwiązań. Nie jest potrzebne żadne dodatkowe narzędzie, aby stworzyć w pełni gotowy i bezpieczny system informatyczny. Rozwiązania automatyzujące zadania i procesy biznesowe tworzone są z użyciem narzędzi drag-and-drop, które nie wymagają umiejętności programistycznych. Dzięki temu systemy mogą być tworzone nawet 5 razy szybciej niż metodami klasycznymi. Ferryt umożliwia użytkownikom biznesowym samodzielne tworzenie procesów, odciążając tym samym działy IT. Intuicyjna obsługa narzędzi sprawia, że zarówno implementacja nowych procesów, jak i ich modyfikacja są łatwe i szybkie. Platforma Ferryt funkcjonuje w największych i najnowocześniejszych instytucjach finansowych w Polsce i zagranicą spełniając wymogi bezpieczeństwa. W okresie kilkunastu lat na platformie zaimplementowano prawie każdy obszar procesowy w bankowości.
Dual Core Fintech Forge	CashMir	Cashmir to uniwersalna platforma, umożliwiająca szybką budowę rozwiązań dla branży Fintech, z wykorzystaniem gotowych i sprawdzonych komponentów, pozwalających znacznie skrócić czas realizacji oraz koszt projektu. Oferowane przez nas oprogramowanie jest wysoce elastyczne i konfigurowalne, aktualnie obejmuje m.in.: – moduł CRM zintegrowany z pozostałymi elementami systemu poprzez liczne automatyzacje – moduł rozliczeń finansowych, traktowany jako księga główna programu – import wyciągów bankowych dla rachunków typu collect z możliwością automatyzacji – integracje z rozwiązaniami Open Banking w zakresie AIS (Kontomatik, Authologic, Transaction Link) – moduł pozwalający na błyskawiczną budowę frontendu/aplikacji dla klienta, zawierającej strefę klienta oraz wspierającej np. proces składania wniosku – integracje z rozwiązaniami zapewniającymi przeprowadzeniem procesów KYC (Blue Media, Authologic, Kontomatik) – płatności online realizowane za pośrednictwem wybranych operatorów płatności – automatyczna wysyłka mail/SMS – scenariusze komunikacyjne z klientem oraz scenariusze windykacyjne – generowanie dowolnych wydruków i plików PDF w oparciu o szablony Word – ocena ryzyka kredytowego, w tym integracje z zewnętrznymi silnikami scoringowymi (SLS, Riskbite) – integracja z system Call Center (Focus Telecom) – cyfrowe podpisy realizowane za pośrednictwem platformy Autenti – integracje z biurami informacji gospodarczej BIG, BIK, CRIF, KRD, KBIG – integracja z Eurotax w zakresie wyceny pojazdów – integracja z systemem E-nadawca Poczty Polskiej – integracja z Bankiem Pocztowym w zakresie czeków GIRO – integracja z platformą do mikro inwestorów Mintos – szereg innych
GFT Poland	Revolutionising personal banking	Zespół GFT Poland zbudował w rekordowym tempie 18 miesięcy architekturę, oprogramowanie i infrastrukturę dostarczania dla pionierskiego, skalowalnego, opartego na chmurze banku wirtualnego Mox, który świadczy usługi bankowości detalicznej całkowicie cyfrowo za pośrednictwem aplikacji mobilnych. We współpracy z inżynierami Mox, firma GFT zaprojektowała bank wirtualny oparty na Vault – wiodącej platformie core banking stworzonej przez Thought Machine. Następnie wdrożyła go w infrastrukturze chmurowej Amazon Web Services. Vault umożliwia klientom tworzenie produktów finansowych z pomocą kodu Pythona i systemu inteligentnych kontraktów. Ta metodyka zapewnia bankowi Mox bezpośrednią własność produktów i możliwość samodzielnego dokonywania zmian. Bank ma obecnie ponad 350 000 klientów i oferuje najnowocześniejsze rozwiązania bankowości detalicznej, w tym w pełni zautomatyzowany proces wdrażania klienta, mechanizmy Machine Learning do przeciwdziałania oszustwom, zaawansowane metody gamifikacji i inne. Klient może otworzyć konto w zaledwie 3 minuty, a uniwersalna karta kredytowa bez numeru zapewnia najwyższy stopień bezpieczeństwa. Jest to pierwszy bank w Hong Kongu, który obsługuje zarówno Apple Pay jak i Google Pay.
HEUTHES	GRYFBANK wersja 21	System GRYFBANK, autorski program HEUTHES, z powodzeniem funkcjonuje w bankowości polskiej od 1993 roku i jest na bieżąco rozwijany i aktualizowany. GRYFBANK zapewnia obsługę całej palety rachunków bieżących, depozytów terminowych i kredytów. Poprzez interfejs graficzny systemu lub w kanałach zdalnych pozwala na realizację operacji we wszystkich krajowych kanałach rozliczeniowych: kartowych, Elixir, SORBNET, Express Elixir, BlueCash, a dodatkowo – po integracji bankowości mobilnej – z usługi BLIK. Pozwala także na obsługę rozliczeń zagranicznych: SEPA, TARGET2, czy bankowość korespondencką poprzez SWIFT. Umożliwia realizację operacji bezgotówkowych i gotówkowych, kasowo-skarbcowych, zleceń stałych i operacji własnych, a także obsługę rejestrów PPP (Przeciwdziałanie Praniu Pieniędzy). Cechą charakterystyczną systemu GRYFBANK jest rozdzielenie księgowości od obsługi produktów bankowych co wpływa na ograniczenie czasu i kosztów niezbędnych do wyszkolenia nowego pracownika obsługi klienta. Do definiowania produktów i reguł nimi rządzących, GRYFBANK zawiera moduł BPCAD (Banking Product Computer Aided Design). Raz zdefiniowany produkt jest wykorzystywany później przy obsłudze klienta, bez potrzeby operowania na kontach; wszelkie księgowania są wykonywane automatycznie w tle. Wraz z GRYFBANK-iem jest dostarczany moduł zarządzania dokumentami DMS, dzięki któremu raporty z systemu mogą być przechowywane w postaci elektronicznej z pieczęcią lub podpisem cyfrowym. DMS może też obsługiwać przepływ dokumentów i formularzy (Workflow). Na życzenie klienta, wraz z GRYFBANK, może również zostać dostarczony moduł ISOF do zarządzania zapleczem banku, zawierający takie podsystemy jak: Kadry-Płace, Środki trwałe, Magazyny (w tym Magazyny – archiwa dokumentów zintegrowane z DMS) i wiele innych. GRYFBANK jest budowany z zastosowaniem zaawansowanych technologii stworzonych przez HEUTHES takich jak: Kobadibus, CADABAT, Client-Web-Serwer, HDB, VIMI, PROAPERMAN, R2O, MODRIBUSMAN, Blockchain Security Module. Architektura bazująca na mikroserwisach stwarza możliwość instalacji i wykorzystania aplikacji w chmurach zarówno prywatnych jak i wynajętych. System jest częścią INFOSTRADY BANKOWEJ – kompleksowego rozwiązania dla bankowości, na który składają się ponadto systemy MULTICENTAUR PAYMENT HUB i GRYFCARD. Łącznie te trzy systemy zapewniają pokrycie znacznego obszaru funkcjonalnego zarówno małego jak i dużego banku. Nowa odsłona systemu przynosi, w wersji 21, nowy interfejs graficzny oparty na przeglądarce internetowej, otwartej architekturze bazującej na mikroserwisach w technologii REST oraz własnej technologii VIMI. GRYFBANK dzięki zastosowaniu szerokiego i otwartego zestawu funkcji API w technologii REST nie tylko wprowadza do banku najnowsze rozwiązania technologiczne, lecz także pozwala na łatwą integrację z innymi systemami. API umożliwia pełną obsługę klienta w bankowości internetowej czy mobilnej, przy zachowaniu pełnego bezpieczeństwa rozwiązania.
Zakład Usług Informatycznych NOVUM	Novum Bank Enterprise NOE	Novum Bank Enterprise NOE to zintegrowany system kompleksowej obsługi banku. Dzięki nowoczesnej technologii, efektywnej architekturze, daleko idącej automatyzacji procesów i elastyczności konfiguracji, użytkownicy uzyskują łatwe kreowanie nowoczesnych produktów i wysoki poziom obsługi klientów, przy jednoczesnym zachowaniu wysokiej dostępności, wydajności i bezpieczeństwa. Novum Bank Enterprise NOE gwarantuje obsługę obszarów organizacyjnych banku (centrali i pozostałych placówek), produktów bankowych, czynności operatorskich, działalności księgowej, analitycznej i sprawozdawczej oraz możliwość rozszerzenia o dodatkowe moduły. Graficzny interfejs do front office, back office i pozostałych aplikacji pomocniczych ułatwiają i usprawniają pracę w systemie. Dodatkowo ścisła integracja z bankowością elektroniczną i mobilną (aplikacje Nasz Bank i Novum-13), elektronicznym systemem obsługi procesów Novum EOD oraz siecią bankomatów i recyklerów Novum HOST umożliwia szybką implementację nowych rozwiązań i efektywne zarządzanie usługami.

Ochronić się przed współczesnymi nieznanymi zagrożeniami

W ostatnim czasie celem zaawansowanych, bazujących na sztucznej inteligencji ataków, jest infrastruktura krytyczna. Szczególnie mocno przestępcy interesują się branżą ochrony zdrowia, IT, usługami finansowymi i energetyką.

Dużym zagrożeniem dla tych podmiotów jest zwłaszcza oprogramowanie ransomware – jest ono dostępne także w modelu usługowym, co sprawia, że korzystający z niego atakujący mają zapewnione wysokie zyski przy ponoszeniu niskich nakładów.

Zintensyfikowanie ataków to zjawisko będące po części pokłosiem szybkiego rozwoju sieci w wyniku takich procesów jak wzrost popularności pracy zdalnej. Cyberprzestępcy mają coraz większe możliwości wykorzystywania starych i nowych luk w słabych zabezpieczeniach sieci domowych, które łączą się z zasobami firmowymi.

Powstanie i rozwój modelu Ransomware-as-a-Service (RaaS) oraz rozbudowanych zestawów narzędzi do atakowania umożliwia skuteczne działanie mniej zaawansowanym technicznie przestępcom. W przeszłości analitycy z należącej do firmy Fortinet jednostki FortiGuard Labs śledzili głównie kilka najważniejszych grup stosujących ransomware. Obecnie zaś rozwinął się cały ekosystem cyberprzestępczy, z dużą liczbą interesariuszy, a handel złośliwym oprogramowaniem kwitnie na czarnym rynku. Ponadto analitycy z FortiGuard Labs obserwują wzrost liczby jeszcze bardziej destrukcyjnego oprogramowania typu wiperware oraz zagrożeń typu zero-day.

Renee Tarun z firmy Fortinet oraz **Derek Manky z FortiGuard Labs** przedstawiają swoje spojrzenie na temat współczesnych wyrafinowanych cyberzagrożeń, oraz omawiają związane z nimi wyzwania.

Dlaczego ochrona przed nieznanymi zagrożeniami jest trudniejsza niż kiedykolwiek?

Derek Manky: Stają się one coraz większym wyzwaniem, ponieważ rozwijające się sieci stwarzają więcej możliwości cyberprzestępcom. Oczywiście, wiele zagrożeń nadal nadchodzi za pośrednictwem poczty elektronicznej i z wykorzystaniem mechanizmów inżynierii społecznej, co jest rozpoznanym problemem, ale to te zagrożenia, o których jeszcze nic nie wiemy, stanowią większe wyzwanie.

Renee Tarun: Zgadzam się – wiele firm nie wie, jakie mogą być źródła zagrożeń w ich środowiskach sieciowych. Na przykład złośliwy kod typu zero-day może pochodzić z rozwiązań funkcjonujących w infrastrukturze IT użytkownika, dlatego po przeprowadzeniu odpowiednich analiz należy skupić się na ograniczaniu ryzyka ataku i planowaniu zabezpieczeń. Ponadto wiele przedsiębiorstw nie ma wystarczającej liczby pracowników i ilości zasobów zapewniających ochronę. Sytuację komplikują też coraz częściej pojawiające się nieznane zagrożenia.

Na czym polega różnica między zapobieganiem zagrożeniom, ochroną przed nimi i łagodzeniem ich skutków?

Derek Manky: Zapobieganie i ochrona to środki tymczasowe. Nawet jeśli uda się zatrzymać zagrożenie, można założyć, że wkrótce ono powróci. W tej sytuacji musimy skłaniać się ku ograniczaniu ryzyka i wykrywaniu zagrożeń zero-day bazując na strategii ochrony warstwowej. Jej dużą częścią jest zapewnienie sobie możliwości głębszej analizy, z ochroną w czasie rzeczywistym. Jeśli firma nie ma rozwiązania typu sandbox in-line, to złośliwe oprogramowanie jest wykrywane dopiero po kilku minutach lub godzinach, a przez ten czas szkody mogły już zostać wyrządzone.

Renee Tarun: Można również pracować nad wykrywaniem i powstrzymywaniem zagrożeń przy użyciu tzw. mechanizmów zwodniczych. W tym przypadku, gdy przestępca wejdzie do sieci lub z niej wyjdzie, uruchamia pułapkę, dzięki której informacja o tym fakcie trafia do administratorów. A jeśli chodzi o łagodzenie niektórych zagrożeń, to należy prowadzić szkolenia z zakresu cyberhigieny wśród pracowników.

> Powstanie i rozwój modelu Ransomware-as-a-Service (RaaS) oraz rozbudowanych zestawów narzędzi do atakowania umożliwia skuteczne działanie mniej zaawansowanym technicznie przestępcom.

W jaki sposób czas obecności złośliwego oprogramowania w systemie wpływa na wyzwania, przed którymi stają dziś osoby odpowiedzialne za bezpieczeństwo?

Derek Manky: Czas, przez który zagrożenie może utrzymywać się w systemie, jest często zdecydowanie zbyt długi. Innym czynnikiem, o którym mówimy w raporcie Threat Landscape Report, jest czas liczony od momentu pojawienia się nowego zagrożenia lub exploita w środowisku IT do momentu, w którym jest on uzbrojony. I nie mówimy już teraz o tygodniach, ale o czasie od 24 do 48 godzin, w trakcie których trzeba zareagować. Cały łańcuch ataku odbywa się teraz znacznie szybciej. Krótszy jest czas od wejścia do systemu do wyjścia z niego. Sprawia to, że firmy potrzebują zautomatyzowanych narzędzi ochronnych, które mogą wykryć te działania.

Renee Tarun: Jeśli o czymś nie wiemy, to nie możemy tego naprawić. Musimy zapewnić sobie odpowiednie możliwości monitorowania sieci i wykrywania zagrożeń, aby rozpoznać, kiedy dochodzi do incydentu związanego z bezpieczeństwem.

Zachować najwyższy poziom bezpieczeństwa i przestrzegać zasad wynikających z regulacji prawnych

IT w sektorze bankowym i firmach świadczących usługi z zakresu wytwarzania oprogramowania dla instytucji z sektora bankowego się zmienia. Głównym motorem tych zmian jest konkurencja i chęć osiągania jak najlepszego wskaźnika „time-to-market".

Zenon **Biedrzycki**
dyrektora Biura Projektowania i Architektury Rozwiązań CyberSecurity, Bank BNP Paribas

Instytucje finansowe musiały postawić na zwinne zespoły IT, które będą w stanie spełniać terminowo wyśrubowane oczekiwania biznesu w zakresie nowych aplikacji i funkcji w istniejącym oprogramowaniu. Analogiczne oczekiwania pojawiły się w stosunku do dostawców oprogramowania.

Kluczowym elementem tych zmian jest odchodzenie od kaskadowych metodyk projektowych z 2-4 dużymi wdrożeniami w ciągu roku, na rzecz metodyk zwinnych, w ramach których praktykuje się nawet kilka wdrożeń w miesiącu. Zmiany te były i są możliwe głównie dzięki zmianom technologicznym, gdzie istotną rolę ogrywają technologie microserwisowe.

Kontrola bezpieczeństwa w procesie

Zmiany w podejściu do rozwoju oprogramowania pociągnęły za sobą także modyfikacje w zakresie dokładania kontroli bezpieczeństwa w procesie. Zespoły wytwórcze zaczęły wymagać także od bezpieczeństwa zwinności i automatyzacji. Ograniczenie zaangażowania przedstawicieli bezpieczeństwa w projekt, polegające na zdefiniowaniu wymagań dla całej aplikacji, weryfikacji ich spełnienia oraz ewentualnego przeprowadzenia audytów bezpieczeństwa i/lub testów penetracyjnych (pentestów) tej aplikacji, przestało przystawać do procesów zwinnych, a wręcz często zaczęło być klasycznym „blokerem" dla dotrzymania terminów wdrożenia.

Zapewnić odpowiedni poziom bezpieczeństwa

Obecnie, zapewnienie odpowiedniego poziomu bezpieczeństwa oprogramowania to już zdecydowanie inne zagadnienie. Wymagania bezpieczeństwa oraz pentesty ograniczają się do konkretnych fragmentów oprogramowania dostarczanych w ramach danego sprintu i co za tym idzie, są one bardziej precyzyjne i nastawione na weryfikację dokładnie tego, co jest wprowadzane w danej zmianie, a nie całości oprogramowania. Pentesty dla jednego formularza modyfikowanego w ramach danej zmiany trwają zdecydowanie krócej niż dla całej aplikacji. W niektórych przypadkach można wręcz ten element pominąć, polegając na wskazaniach skanerów. Testy penetracyjne w pełnym zakresie funkcji aplikacji są natomiast realizowane w cyklu rocznym lub dwuletnim, po uprzednim zaplanowaniu i nie wpływając na procesy zwinnego wytwarzania oprogramowania.

Kluczowe zagadnienia

Kluczowe z perspektywy automatyzacji weryfikacji bezpieczeństwa w procesach wytwórczych są skanery bezpieczeństwa wykorzystywane przez zespoły wytwórcze. Zespół, niezależnie czy jest to zespół instytucji finansowej, czy też podmiotu wytwarzającego oprogramowanie dla instytucji finansowych, powinien stosować i respektować błędy i podatności wskazywane przez skanery typu:

- SAST (Static Application Security Testing),
- dedykowany do statycznej analizy kodu źródłowego,
- często nielubiany przez programistów, ze względu na ilość błędów i false-positive,
- czasami mylony także ze skanerami, których priorytetem jest zapewnienie jakości kodu,
- SCA (Software Composition Analysis),
- dedykowany do identyfikacji komponentów otwartoźródłowych, weryfikacji podatności w tych komponentach oraz ewentualnych problemów związanych z postanowieniami licencyjnymi, na podstawie których można bądź nie, wykorzystać komponent,
- często przysparzający sporo problemów programistom, ponieważ wymaga od nich regularnego podnoszenia wersji komponentów otwartoźródłowych i weryfikacji nowych podatności w tych komponentach (pojawiających się w trakcie działania oprogramowania) pod kątem ich wpływu na oprogramowanie,
- DAST/IAST (Dynamic Application Security Testing / Interactive Application Security Testing),
- dedykowany do automatycznego skanowania działającej aplikacji, wykrywający błędy w działającym oprogramowaniu,
- stosowany przez uruchomienie nowej wersji, ale także w trakcie działania oprogramowania,
- automatyzujący częściowo kontrole, które można zrealizować w ramach pentestów, ale w żadnym wypadku niezastępujący w pełni testów dla kluczowych zmian w aplikacji i okresowo realizowanych testów penetracyjnych w pełnym zakresie funkcji aplikacji.

Właściwe praktyki bezpieczeństwa

Nie bez znaczenia są tu także właściwe praktyki bezpieczeństwa związane np. z repozytoriami kodu, repozytoriami artefaktów, repozytoriami stanowiącymi proxy do publicznych repozytoriów komponentów otwartoźródłowych.

Instytucja finansowa podejmując współpracę z dostawcą w zakresie oprogramowania, które może mieć istotny wpływ na organizację i jej procesy, chce mieć pewność, że będzie ono rozwijane w sposób zapewniający co najmniej analogiczny poziom bezpieczeństwa jak oprogramowanie rozwijane w banku. Jeżeli w ramach umowy nie ma zagwarantowanego dostępu do kodu źródłowego, instytucja finansowa zapewne poprosi o dostarczenie odpowiednich raportów potwierdzających efektywne wykorzystanie oprogramowania typu SAST. Jeżeli umowa przewiduje dostęp do kodu źródłowego, zostanie on poddany weryfikacji skanerem typu SAST i ewentualnie dodatkowym przeglądom, a znalezione błędy zostaną przekazane do dostawcy celem ich usunięcia bądź oceny z perspektywy ryzyka w kontekście oprogramowania.

Zapewne analogicznie instytucja finansowa będzie działać w zakresie komponentów otwartoźródłowych, o ile takie komponenty występują w oprogramowaniu. Tu do skanowania, w zależności od technologii, będą potrzebne określone artefakty, bądź wystarczą same komponenty instalacyjne oprogramowania. Wynik skanowania pokaże podatności i ewentualne ryzyka wynikające z zapisów licencji komponentów otwartoźródłowych. Naruszenia zdefiniowanych przez bank polityk powinny być zinterpretowane przez dostawcę i ewentualnie usunięte bądź wyjaśnione.

Przestrzegać odpowiednich standardów

Wytwarzając oprogramowanie dla instytucji finansowych, należy liczyć się także z kilkoma innymi zasadami i weryfikacjami, którym takie oprogramowania zostanie poddane. Testy penetracyjne po uruchomienie aplikacji, przeprowadzane przez pentesterów i z wykorzystaniem automatycznych skanerów, mogą pokazać podatności w samej konfiguracji środowiska, ale mogą pojawić się także podatności, których usunięcie będzie wymagało zaangażowania dostawcy. Dodatkowo bank może, a wręcz powinien wymagać, żeby oprogramowanie było budowane z przestrzeganiem odpowiednich standardów w zakresie podatności i hardeningu, sprowadzających się do np. instalacji oprogramowania na utwardzonych i niepodatnych obrazach systemów operacyjnych, wyposażonych już w odpowiednie narzędzia bezpieczeństwa (np. AV, EDR), czy w przypadku technologii microserwisowych stosowania tzw. obrazów bazowych, które przed dopuszczeniem do użycia także poddawane są procesom utwardzania. Istotne mogą być także platformy programistyczne (frameworki), które muszą być spójne ze standardami architektonicznymi banku. Nie bez znaczenia, z perspektywy bezpieczeństwa, będą ważne także takie aspekty jak zastosowanie, tam, gdzie jest to zasadne, wieloskładnikowego uwierzytelnienia (Multi-Factor Authentication, MFA) czy odpowiednie przechowywanie haseł, gwarantujące poufność tych danych w całym procesie wdrożenia i działania oprogramowania.

Banki pełnią funkcję instytucji zaufania publicznego i muszą dbać o to, żeby to zaufanie nie zostało nadszarpnięte przez niewłaściwe kontrole w zakresie wytwarzania i wdrażania oprogramowania dostarczanego przez dostawców. Niezależnie od tego, czy oprogramowanie jest rozwijane w infrastrukturze banku, czy w infrastrukturze dostawcy, weryfikacje bezpieczeństwa powinny być zbliżone i ewentualnie zróżnicowane z perspektywy istotności danego oprogramowania, a nie z perspektywy tego, kto rozwija dane oprogramowanie i jakie kontrole ma wdrożone w procesie wytwórczym.