OPROGRAMOWANIE DLA FIRM

Tylko DMS? A może jednak szerszy workflow

W dzisiejszych czasach DMS jest często elementem szerszego zestawu funkcji zawartych w rozwiązaniach typu workflow (ang. przepływ pracy). Przykładem są systemy, które z jednej strony zawierają typowe funkcje DMS, tj. elektroniczne gromadzenie, indeksowanie, udostępnianie i wyszukiwanie różnego rodzaju dokumentów powstających w firmie lub też przychodzących do niej z zewnątrz, a z drugiej rozszerzają je o możliwość obsługi procesów przepływu dokumentów do poszczególnych działów i osób oraz o rozwiązania z zakresu CRM. Systemy takie zapewniają także wsparcie dla definiowania i wysyłania w obieg formularzy oraz zawierają szereg narzędzi umożliwiających prowadzenie efektywnej pracy grupowej.

Wojciech **Grzybek**

Rozwiązania klasy workflow oprócz obsługi obiegu dokumentów i pracy dzięki definiowaniu i odwzorowaniu struktury organizacyjnej firm i grup pracowników oraz ich ról w jednostkach organizacyjnych spełniają również funkcje wirtualnego dysku twardego. W tym zakresie ważne miejsce zajmuje firmowa poczta elektroniczna.

CRM – na czym polega?

Dzięki temu, że jest ona obsługiwana w systemach workflow, wszystkie wiadomości przychodzące i wychodzące z firmy, zarówno z ogólnych, jak i indywidualnych kont pocztowych są zgromadzone w jednym systemie i mogą być dostępne innym osobom z zachowaniem odpowiednich uprawnień oraz zastępstw. W najnowszych rozwiązaniach tej klasy zawarte są również rozwiązania z zakresu CRM. Niektórzy producenci pod tym pojęciem rozumieją nie tylko klasyczne rozwiązania w zakresie rejestracji, zarządzania i analizy wszystkich zdarzeń z klientami, ale również funkcje prognozowania umożliwiające zaplanowanie sprzedaży, określenie sposobu osiągnięcia założonych celów oraz bieżące śledzenie ich realizacji. Tak zbudowane systemy ułatwiają również pracownikom oraz kadrze menadżerskiej organizację, planowanie i zarządzanie zadaniami oraz kontrolę czasu i kosztów ich wykonywania.

Zabezpieczenia i inne udogodnienia

Ciekawą funkcją, którą wnoszą nowoczesne systemy workflow pracujące w przeglądarce, jest możliwość pracy on-line z dokumentami pakietów biurowych LibreOffice oraz Microsoft Office. Z kolei możliwość dodania do dokumentów, wprost w systemie, pieczęci cyfrowej powoduje, że dokumenty te stają się zabezpieczone. Pieczęć cyfrowa, w odróżnieniu od podpisu cyfrowego, może być w firmie przypisana do wielu osób, ułatwiając obieg pracy grupowej. Pracę grupową mogą wspierać zawarte w systemach workflow wirtualne przestrzenie pracy, do których użytkownik zaprasza inne osoby i grupy i w której umieszcza dokumenty elektroniczne do wspólnego opracowania. System workflow powinien także obsługiwać mechanizm zastępstw niwelując zakłócenia związane z nieobecnością pracowników w firmie. Funkcje systemowe w tym zakresie udostępniają dokumenty zastępcom bądź też rozdzielają dokumenty pomiędzy wieloma zastępcami lub grupami osób zgodnie z regułami.

Dodatkowe funkcje

Klienci powinni wybierać rozwiązania, w których znajduje się rozbudowany moduł definiowania, wysyłania w obiegi, wypełniania i raportowania formularzy. Dzięki niemu bardzo łatwo można wysłać, odebrać i przetworzyć dowolną ilość informacji krążących pomiędzy dużą liczbą osób, w firmach i instytucjach o złożonej i rozproszonej strukturze. System workflow powinien mieć możliwość integracji z zewnętrznym portalem WWW, który umożliwi klientom firmy bezproblemowe udostępnianie przez Internet dokumentów elektronicznych, a także dokumentów wewnętrznych systemu workflow. Rzadko spotykaną funkcją w systemach tego typu jest możliwość współpracy workflow z dowolnym systemem finansowo-księgowym. Taka funkcja wspomaga przygotowanie dekretów księgowych na podstawie zbiorów dokumentów elektronicznych gromadzonych w systemie.

Autor jest prezesem zarządu HEUTHES Sp. z o.o.

GAZETA FINANSOWA
16 – 22 września 2016 r.
BIZNES RAPORT

Pomocy, wirus w moim komputerze!

XXI wiek oraz dynamiczny rozwój sieci Internetu urzeczywistniły scenariusze filmów akcji, w których na porządku dziennym bohaterowie dokonują włamań do serwerów przeciwnika. Niestety łatwość z jaką im to przychodzi nie jest daleka od rzeczywistości.

Sebastian **Jarosik**

Działające w internetowym podziemiu najzdolniejsze jednostki poświęcają swój czas na odkrywanie luk bezpieczeństwa w systemach informatycznych. Chcąc zaprezentować swoje umiejętności i posiadaną wiedzę tworzą dedykowane narzędzia służące do przeprowadzania włamań. Duża ich część jest upubliczniana i może posłużyć do przeprowadzenia skutecznego ataku nawet przez średnio zaawansowanego użytkownika komputera. Takie działanie może doprowadzić zarówno do zatrzymania pracy systemu, jak i do kradzieży przepływających przez niego danych, stanowiących tajemnicę danej osoby lub przedsiębiorstwa.

Luki w systemie

Najpowszechniejszą przyczyną takich ataków jest chęć uzyskania korzyści majątkowych. Mogą one pochodzić ze sprzedaży wykradzionych tajemnic handlowych, jak dane klientów i kontrahentów, ceny zakupu towarów i surowców czy ceny sprzedaży. Powszechnym działaniem jest również żądanie okupu za odblokowanie zatrzymanego przez cyberprzestępców serwera lub powstrzymanie się od działania mogącego doprowadzić do utraty reputacji – np. publikacja zdobytych informacji czy też możliwość podmiany treści na przejętym serwerze. Dlaczego więc tak duża część oprogramowania posiada wady, którymi są luki bezpieczeństwa? Przyczyn jest wiele, a główną z nich jest poziom zaawansowania dzisiejszego oprogramowania. Twórcy aplikacji korzystają z wielu elementów, które zostały już wcześniej wytworzone przez innych autorów. Mogą to być zarówno ogólnodostępne tzw. biblioteki programistyczne udostępnione jako wolne oprogramowanie lub fundamenty niezbędne do działania aplikacji tworzone od wielu lat przez największe korporacje (takie jak Microsoft Windows czy Oracle Database). Ostatecznie widziana przez nas jako monolityczny twór prosta aplikacja, okazuje się być skomplikowaną strukturą informatyczną posiadającą niezliczoną liczbę autorów. Niestety luka w którymkolwiek z elementów składowych umożliwia uzyskanie niepowołanego dostępu do systemu.

Aktualizuj, aby uniknąć ataku

Jedną z najbardziej znanych praktyk informatycznych jest ta mówiąco o konieczności aktualizacji oprogramowania. Nowe wersje aplikacji nie tylko dodają nowe funkcjonalności, lecz również niwelują nowo odkryte podatności na ataki cyberprzestępców. Pamiętajmy o zinwentaryzowaniu wszystkich elementów bazowych naszej aplikacji (system operacyjny, baza danych, firmware serwera) oraz o ich aktualizacji. W dużej części próby przejęcia systemu informatycznego będą odbywać się przez sieć. Mając tego świadomość zadbajmy o odpowiednie zabezpieczenia tego wektora ataku. Na rynku dostępnych jest wiele zaawansowanych rozwiązań, które oprócz podstawowych funkcji popularnego firewalla potrafią uruchamiać przesyłane pliki (tzw. sandboxing). W praktyce wygląda to w ten sposób, iż wspomniany skaner uruchamia przesyłany plik jeszcze zanim zostanie on przekazany do użytkownika. Takie kontrolowane uruchomienie symulujące użytkownika potrafi poddać zawartość transmisji ocenie i na jej podstawie zadecydować czy dokonać blokady niepożądanej treści. Tego typu rozwiązania są wydajniejsze i umożliwiają bardziej wnikliwą analizę aniżeli programy antywirusowe instalowane na komputerach użytkowników końcowych czy też na serwerach.

Firma zewnętrzna czy informatyk w firmie?

Dynamiczny rozwój informatyki sprawił, iż każde przedsiębiorstwo posiada własny wewnętrzny lub zewnętrzny (outsourcing) zespół administratorów systemów informatycznych. Należy mieć na uwadze, iż niezależnie od stopnia zaawansowania członków zespołu ich praca powinna podlegać cyklicznej weryfikacji w obszarze bezpieczeństwa informatycznego. Wiedza dot. cyber security dezaktualizuje się bardzo szybko. Niedostosowanie się w porę do obowiązujących standardów może oznaczać wymierne straty dla naszej organizacji. Coroczny audyt bezpieczeństwa zlecony specjalistycznemu dostawcy tego typu usług pomaga zaktualizować wiedzę zespołu, procedury oraz podnieść poziom bezpieczeństwa. Warto rozważyć skorzystanie z usług firmy zewnętrznej w obszarze monitoringu bezpieczeństwa informatycznego – tzw. Security Operations Center. Inżynierowie specjaliści pracujący w SOC wspomagani przez dedykowane oprogramowanie mają za zadanie analizować informacje generowane przez wszystkie urządzenia informatyczne w sieci danego przedsiębiorstwa (komputery, serwery, switche, routery, firewalle, drukarki i inne). Posiadają oni odpowiednią wiedzę i narzędzia, aby wykrywać i odpierać próby ataków w sposób ciągły 24 godziny na dobę. W niedalekiej przyszłości takie usługi będą tak samo powszechne, jak wynajem pracowników ochrony fizycznej.

Uważaj co „klikasz"

Na koniec pamiętajmy, że najsłabszym ogniwem możemy okazać się my sami. Wielu cyberprzestępców wykorzystuje socjotechniki celem przejęcia kontroli nad naszym komputerem. Mowa tu w głównej mierze o wiadomościach poczty elektronicznej, wiadomościach przesyłanych przez komunikatory internetowe, czy też o nośnikach danych przesyłanych pocztą tradycyjną. Zwracajmy uwagę na to, czy nadawca otrzymanego e-maila, pendrive'a lub płyty CD jest nam znany, czy jego dane są poprawne (czy np. adres e-mail nie ma literówki upodabniającej go do innego zaufanego adresu), czy nie następuje próba podszycia się pod znaną nam osobę lub potencjalnego kontrahenta. W otrzymanym pliku lub w załączonym linku do strony www może znajdować się złośliwe oprogramowanie, które umożliwi przejęcie kontroli nad naszym komputerem. Znane są również przypadki rozmów telefonicznych, które służą uwiarygodnieniu treści fałszywej wiadomości. W razie wątpliwości zawsze warto przekazać podejrzaną zawartość służbom informatycznym celem dokonania analizy.

Autor jest network, linux & security business unit managerem w Exorigo-Upos Sp. z o.o.

Skutecznie zabezpieczyć się przed atakami hakerów

Z Davidem Klusackiem, dyrektorem Check Point Software Technologies w Europie, rozmawiała Joanna Zielińska

Jak wygląda obecnie sytuacja światowego cyberbezpieczeństwa?

Check Point w ostatnim czasie zidentyfikował ponad 2400 aktywnych rodzin malware. To blisko 60 proc. wzrost względem danych z przełomu roku. Na świecie co 4 sekundy dochodzi do ściągnięcia pliku malware typu zero-day, natomiast co pół godziny dochodzi do wycieku wrażliwych danych z organizacji. Cyberprzestępcy są coraz bardziej wyrafinowani – poszukują luk w systemach zabezpieczeń, wykorzystują nieuwagę pracowników… W 2015 roku 88 proc. firm padło ofiarami skutecznych ataków, które kosztowały je średnio 3,79 mln USD (23 proc. wzrost w stosunku do 2014 r.). Generalnie, wraz z rozwojem technologii i tzw. Internetu rzeczy (internet-of-things), hakerzy posiadają coraz więcej możliwości ataku…

Na co firmy powinny zwrócić uwagę, chcąc bezpiecznie funkcjonować?

Współczesne przedsiębiorstwa muszą stawić czoła wyzwaniu, jakie niesie ze sobą zabezpieczenie pracowników zdalnych, korzystających często z prywatnych urządzeń, wykorzystując aplikacje oparte na chmurze. Stale wzrasta również liczba tzw. sieciowych punktów wejścia (entry point), wymagających solidnej ochrony w firmie… należy zatem zwrócić uwagę, by każdy – zarówno przewodowy, jak i bezprzewodowy – punkt wejścia, jak również serwery czy narzędzia mające zapewnić ich bezpieczeństwo, były stale aktualizowane. Aktualność systemów zabezpieczających była w zeszłym roku jednym z największych niedopatrzeń, których dopuściły się organizacje i firmy na całym świecie.

Czy sposób działania hakerów zmienia się na przestrzeni lat?

Hakerzy szukają coraz to nowszych sposobów na przejęcie wrażliwych danych. Wydaje się, że rola konwencjonalnych typów złośliwego oprogramowania może powoli spadać, jednak wzrastać będzie zagrożenie mobilnymi rodzinami malware – to właśnie urządzenia przenośne bywają często najsłabszym ogniwem sieci firmowych. Zmieniają się nie tylko narzędzia, lecz również sposób funkcjonowania grup hakerskich. Od jakiegoś czasu obserwujemy wzrost trendu ransomware-as-a-service, czyli hakerskich usług związanych z e-okupami. Twórca rekrutuje swoich partnerów, którzy dystrybuują oprogramowanie w zamian za udział w zyskach. Taka taktyka pozwala na szersze rozpowszechnienie malware i generowanie wyższych zysków.

BIZNES RAPORT
GAZETA FINANSOWA
16 – 22 września 2016 r.

Jak zapewnić firmie bezpieczeństwo podatkowe po 1 stycznia 2017 r.?

Za niewiele ponad 3 miesiące małe i średnie firmy obudzą się w nowej rzeczywistości prawnej. Z dniem 1 stycznia wchodzi nowy obowiązek podatkowy dotyczący raportowania ewidencji VAT w formacie Jednolitego Pliku Kontrolnego.

Obowiązek raportowania danych finansowych w formie Jednolitego Pliku Kontrolnego objął tzw. duże przedsiębiorstwa już od 1 lipca. Wstępne szacunki mówią, że pierwsze obowiązkowo wysłane raporty (VAT JPK) wysłało do urzędów skarbowych ok. 6 tys. firm. Ministerstwo Finansów szacuje, iż m.in. dzięki elektronicznym kontrolom znacznie wzrosła skuteczność ściągalności podatków. W ciągu pierwszych sześciu miesięcy 2016 r. wykryto wypłaty nienależnego zwrotu VAT na kwotę 832 mln zł. W porównaniu do analogicznego okresu 2015 r. wartość ta wzrosła aż o 71,3 proc.

Wzmożone i dokładniejsze kontrole wymusiły także na podatnikach korekty deklaracji. Ich liczba w pierwszej połowie tego roku wzrosła aż o 270,5 proc. w porównaniu do analogicznego okresu roku ubiegłego. Łączna kwota korekt deklaracji wyniosła 336,6 mln zł. Wzrosła także liczba wpłat – do poziomu 566,5 mln zł (wzrost o 35,7 proc.). Z kolei łączna kwota zatrzymanych z budżetu wypłat z tytułu zwrotu VAT wyniosła 266 mln zł (wzrosty o 288,3 proc.).

Fiskus może liczyć na jeszcze większe uszczelnienie systemu vatowskiego od 2017 r. Od początku przyszłego roku obowiązek raportowania VAT JPK obejmie małe i średnie firmy. Niedopełnienie tego obowiązku wiąże się z konsekwencjami finansowymi. Ok. 170 tys. firm sektora MSP na przystosowanie swoich systemów księgowo-rachunkowych do wymogów JPK ma czas tylko do końca roku.

Szokujące kary za niedotrzymanie terminów podatkowych

Plik JPK należy przesyłać łącznie z deklaracją VAT, czyli do 25. dnia kolejnego miesiąca, nawet jeśli VAT rozlicza się kwartalnie. Niedotrzymanie terminowego obowiązku przesyłania informacji może być potraktowane przez urzędy skarbowe jako naruszenie obowiązku podatkowego. Raporty w formie pliku JPK są bowiem informacjami podatkowymi, dlatego nieprzesłanie ich w terminie stanowi naruszenie art. 80 Kodeksu karnego skarbowego i może być zakwalifikowane jako przestępstwo skarbowe lub wykroczenie skarbowe.

Jeżeli niedotrzymanie ustawowego obowiązku zostanie uznane za przestępstwo skarbowe, podatnikowi grozi grzywna w wysokości od 10 do 120 stawek dziennych w wysokości nie mniejszej niż 1/30 minimalnego wynagrodzenia za pracę i nie większej niż jej czterystukrotność. Może zatem wynosić od 616,60 zł do 2 959 680 zł. Jeśli zaniedbanie przedsiębiorcy zostanie zakwalifikowane jako wykroczenie, może on zostać obciążony grzywną w wysokości od 1/10 do dwudziestokrotności wysokości minimalnej pensji. Jeżeli grzywnę orzeka sąd, może ona wynieść od 185 zł do 37 000 zł. Grzywna nakładana mandatem karnym może wynieść maksymalnie 3 700 zł. Karą pieniężną może zostać obciążona osoba zajmująca się sprawami gospodarczymi w firmie, szczególnie finansowymi. Nie tylko osoba decyzyjna, zajmująca kierownicze stanowisko czy prowadząca działalność, ale także pracownik, któremu został powierzony obowiązek przygotowania i przesłania raportu. Jednak ostateczna decyzja o przyznaniu takiej osobie grzywny zależy m.in. od treści umowy łączącej ją z firmą, zakresu i możliwości realizacji obowiązków czy też okoliczności danej sprawy.

Jak uniknąć grzywny?

Mali i średni przedsiębiorcy na przygotowania do nowego obowiązku podatkowego mają coraz mniej czasu. W ciągu najbliższych kilku tygodni warto zaopatrzyć się w odpowiednie oprogramowanie, za pomocą którego można wygenerować odpowiedni plik kontrolny. Jednakże by zapewnić sobie maksimum bezpieczeństwa prawnopodatkowego warto pójść krok dalej. Samo wytworzenie przez program pliku JPK może tego nie zagwarantować. Przed wysłaniem danych do urzędu skarbowego korzystnie jest sprawdzić poprawność pliku – nie tylko pod względem technicznym, ale także merytorycznym. Taką możliwość daje platforma Sage e-Audytor, na której można dokonać weryfikacji plików kontrolnych pod kątem spójności matematycznej oraz kompletności pojedynczego pliku. Ponadto platforma daje możliwość sprawdzenia poprawności logicznej i merytorycznej plików. W kontekście nowego obowiązku związanego z raportowaniem VAT należy wspomnieć o możliwości porównywania wygenerowanego raportu VAT JPK z deklaracją VAT-7. Dopiero po dokonaniu takich analiz można być pewnym, że dane podatkowe są poprawne i bez obaw przesyłać je do urzędu skarbowego.

GAZETA FINANSOWA
16 – 22 września 2016 r.
BIZNES RAPORT

W PUDEŁKACH I CHMURZE

Okres szybkiego rozwoju i popularności systemów ERP rozpoczął się w latach 90. ubiegłego wieku. Początkowo systemy ERP dostępne były – ze względu na cenę – tylko dla dużych firm. Dzisiaj, nawet małe przedsiębiorstwa mogą pozwolić sobie na system o bogatej funkcjonalności.

Jakub **Czyżkowski**

Systemy ERP różnią się między sobą w zależności od przeznaczenia. Najmniejsze, zwane powszechnie „pudełkowymi", przeznaczone są do masowej dystrybucji, a korzystają z nich głównie bardzo małe przedsiębiorstwa. Systemy takie projektowane są tak, aby mogły być wykorzystywane przez bardzo duże grono firm, a więc z definicji o podobnych wymaganiach. „Pudełkowe" oprogramowanie to raczej systemy do prowadzenia ewidencji dokumentów gospodarczych, niż realne narzędzia wspomagające zarządzanie.

Kto sięga po ERP

Gdy liczba osób korzystających z programu przekracza kilkanaście osób, pojawia się naturalna konieczność wsparcia organizacji ich pracy. Wówczas systemy „pudełkowe" przestają wystarczać. Firmy sięgają wtedy po bardziej zaawansowane rozwiązania z tak zwanej „średniej półki". Systemy tej klasy można nazwać prawdziwymi systemami ERP, ponieważ często implementują zaawansowane funkcje planowania na poziomie taktycznym (planowanie zakupów, sprzedaży, planowanie dystrybucji czy produkcji, planowanie przepływów finansowych itp). Średnie firmy nastawione są na szybki rozwój i konkurencyjną walkę. Często odważnie poszukują wzrostu efektywności i wydajności. Wówczas uniwersalne narzędzia, nawet te szeroko konfigurowalne, są zbyt „ociężałe". Wdrożenie zmian zajmuje zbyt wiele czasu i jest złożoną czynnością.

Dla każdego coś dobrego

Często by poradzić sobie z ograniczeniami, wewnętrzny zespół programistów dopisuje potrzebne funkcjonalności. System „obrasta" różnymi „przystawkami". Po jakimś czasie firma przestaje się orientować w tak powstałym bałaganie i przychodzi czas na kolejną zmianę. Są systemy przeznaczone dla średnich i dużych firm, które oprócz bogatej funkcjonalności ERP oferują bardzo elastyczne środowisko budowania i rozwijania funkcjonalności specyficznych dla konkretnej firmy. Takie narzędzia nie są najtańsze, ale w średnich i dużych firmach przynoszą znacząco większe korzyści niż koszty. A chmura? W każdym powyższym segmencie można znaleźć producentów oferujących swoje rozwiązania w chmurze. Na „chmurę" decydują się często firmy mniejsze lub takie, które zakładają okres eksploatacji oprogramowania krótszy niż 3 lata. Jeśli okres użytkowania ma być dłuższy, to własna infrastruktura jest zazwyczaj bardziej opłacalna.

Autor jest wiceprezesem zarządu Sente Systemy Informatyczne sp. z o.o.

Zanim wybierzesz system ERP

System ERP to inwestycja w przyszłość – może się wydawać, że wdrożenie takiego systemu to zmiana głównie technologiczna, ale w istocie jest to prawdziwe przeorganizowanie pracy w firmie.

Katarzyna **Jeznach**

Rozmowy o wdrożeniu systemu ERP zaczynają się zwykle z określonych powodów: pracownicy mają problem z wykonywaniem swoich obowiązków, bo dotychczasowe rozwiązania okazują się niewystarczające, a w firmie nastąpiły istotne zmiany, np. rozszerzenie działalności itd. Wypisanie i uporządkowanie tych powodów, a następnie przypisanie im odpowiednich priorytetów będzie bardzo pomocne w dalszych etapach pracy nad wyborem oprogramowania. Nowoczesne systemy ERP są kompleksowymi, często bardzo zaawansowanymi systemami IT, składającymi się z wielu modułów, dlatego lista z najważniejszymi oczekiwaniami wobec nowego rozwiązania pozwoli ocenić system pod kątem takich właśnie funkcjonalności, bez nadmiernego koncentrowania się na elementach, które na tym etapie działalności firmy nie będą miały kluczowego znaczenia.

Jakie cele ma zrealizować system ERP?

Opisanie problemu, np. konieczność wykonywania różnych czynności ręcznie, bez wprowadzonej automatyzacji, czy po prostu – bardzo skomplikowany w obsłudze system, to dopiero pierwszy krok. Następnym jest wyznaczenie celu, najlepiej mierzalnego i określonego w czasie – np. „chcę zautomatyzować proces wymiany dokumentów pomiędzy różnymi działami firmy tak, by dany pracownik zamiast poświęcać na to zadanie 4 godziny tygodniowo, po pierwszych 2 miesiącach pracy z nowym systemem poświęcał na to tylko godzinę". Często celem wprowadzenia systemu ERP może być po prostu konieczność dostosowania się do obowiązujących przepisów prawnych – wówczas warto zwrócić uwagę na takie aspekty jak łatwość pracy z systemem, wykorzystywane technologie, możliwość integracji z innymi rozwiązaniami. Oprogramowanie powinno odpowiadać na potrzeby biznesowe przedsiębiorstwa. Dobry system informatyczny jest elastyczny i dopasowuje się do procedur i struktury organizacyjnej firmy. System ERP powinien umożliwiać nam łatwą integrację z innymi programami np. branżowymi. Dokonując wyboru trzeba brać pod uwagę też technologiczną aktualność systemu oraz dostosowanie go do wymogów polskiego prawa. Najlepsi producenci regularnie dostarczają nowe wersje systemów wraz ze zmianami prawa gospodarczego.

Co z budżetem?

Czyli: jakie nakłady finansowe firma może przeznaczyć na zakup, wdrożenie i utrzymanie nowego systemu? Należy przy tym pamiętać, że cena gotowego rozwiązania to tylko część kosztów, jakie trzeba będzie ponieść. By oprogramowanie faktycznie zostało wdrożone, a pracownicy mogli z niego swobodnie korzystać, należy jeszcze wykonać szereg działań, które odpowiednio kosztują. W rozmowach z klientami, którzy chcą wdrożyć system ERP, najważniejsze jest postawienie pytania: jakie są ich oczekiwania poza samym systemem, czyli te dotyczące integracji ERP z innymi systemami, czy potrzebne będą szyte na miarę rozwiązania programistyczne, jakiej oczekują opieki serwisowej. Klienci potrzebują wsparcia także już po zakończonym wdrożeniu, ponieważ oprogramowanie musi być aktualizowane, ale przede wszystkim chodzi o to, by w razie pytań, wątpliwości, mieli się do kogo zwrócić. Z wdrożeniem systemu ERP wiąże się szereg czynności, wśród których są m.in.:

- analiza przedwdrożeniowa, pozwalająca zbadać potrzeby przedsiębiorstwa,
- wybór i instalacja odpowiedniego systemu,
- konfiguracja systemu tak, by dopasować go do wymagań firmy,
- integracja z pozostałymi systemami w firmie,
- wprowadzenie rozwiązań indywidualnych. W przypadku, gdy nie można zintegrować ze sobą dwóch systemów działających w firmie za pomocą już istniejących rozwiązań,
- szkolenie pracowników, co jest kluczowe, ponieważ system jest tylko narzędziem w rękach odpowiedniej osoby,
- opieka powdrożeniowa, obejmująca m.in. aktualizacje oprogramowania czy możliwość kontaktu z konsultantem w razie jakichkolwiek problemów z systemem.

Przy wyborze firmy wdrażającej system ERP warto sprawdzić, czy będzie ona oferowała usługi w każdym z tych zakresów. Wybór firmy oferującej kompleksowe usługi znacznie ułatwi wdrożenie systemu ERP.

Autorka jest ekspertem DATEV.pl