

# nowe technologie

www.comarch.pl  
MAGAZYN COMARCH  
nr 2/2008 (12)  
ISSN 1734-4212

TEMAT NUMERU

## ZARZĄDZANIE DOSTĘPEM DO SYSTEMÓW IT

- › Przegląd nowoczesnych metod uwierzytelniania i autoryzacji transakcji
- › Uwierzytlenianie i autoryzacja transakcji w dobie urządzeń mobilnych
- › Zarządzanie dostępem i tożsamością w korporacjach
- › Niebezpieczeństwa płynące z sieci wewnętrznej firmy – sposób ochrony

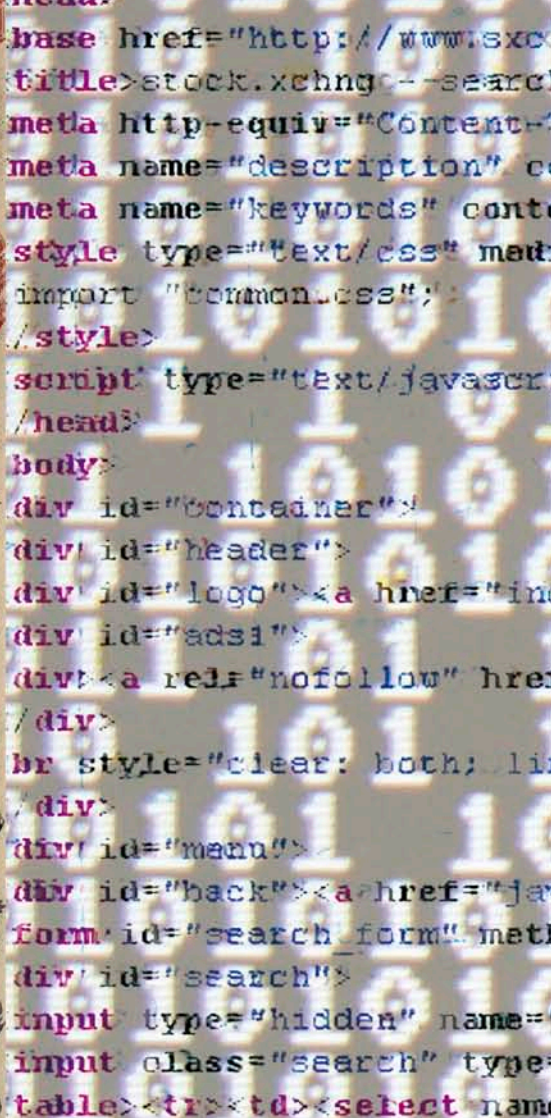
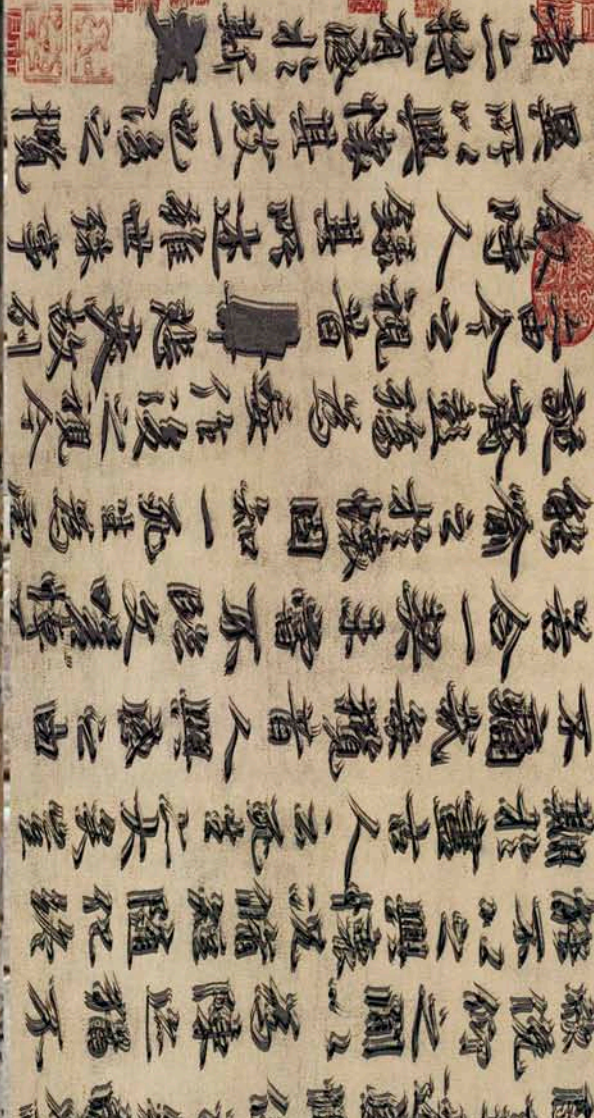
### Rozwiązania i wdrożenia

OCEAN jest Agile

### Trendy i strategie

ITIL – koszt czy wartość dodana?





Język Egipcjan...

Język mieszkańców Japonii...

Język webmasterów...

## COMARCH CMS

Twórz strony www bez znajomości żadnego z nich

więcej na:  
[www.finance.comarch.pl](http://www.finance.comarch.pl)

**COMARCH**  
SYSTEMY INFORMATYCZNE

**Nowe Technologie****Kwartalnik**

numer 2/2008 (12)

**Redaktor Naczelny**

Magdalena Grochala

**Współpraca**

Antoni Sikora

**Skład i grafiki**

Adam Dąbrowski

**Korekta**

Magdalena Grochala

**Projekt**

Maciej Urbaneck

**Wydawca**

Comarch SA

Al. Jana Pawła II 39a

31-864 Kraków

tel.: (12) 64 61 000

fax: (12) 64 61 100

e-mail: pr@comarch.pl

www.comarch.pl

Infolinia: 0 801 33 44 55

**Druk**

Drukarnia Wydawnicza

im. W.L. Anczyca

ul. Wrocławska 53

30-011 Kraków

**Nakład:**

4 500 egz.

**Magazyn Nowe Technologie**

jest wydawnictwem bezpłatnym dostępnym w subskrypcji. Artykuły publikowane w niniejszym wydawnictwie mogą być kopiowane i przedrukowywane za wiedzą i zgodą redakcji. Nazwy produktów i firm wymienione w niniejszym wydawnictwie są znakami handlowymi i nazwami towarowymi odpowiednich producentów.

ISSN 1734-4212



proj. Adam Dąbrowski



2 listopada 1988 roku, około godziny 20:00 Robert Tappan Morris uruchomił i wprowadził do sieci pierwszego robaka, zwanego dziś robakiem Morrisa. Robak w ciągu kilku godzin sparaliżował działanie 10 procent całego ówczesnego Internetu, infekując ponad 6 tysięcy komputerów.

Podobnie jak Alfred Nobel nie zdawał sobie sprawy z przyszłych konsekwencji swojego wynalazku, jakim był dynamit, tak Morris nie przewidział skutków działania swojego robaka. Tworząc składający się z 3 tysięcy linijek kod, Morris chciał pokazać tylko słabości zabezpieczeń stosowanych wówczas systemów operacyjnych. Pobudki może i miał szlachetne, ale realizacja nie dość, że przerosła wyobrażenia pomysłodawcy, to jeszcze była początkiem zmasowanej inwazji szkodliwych robaków na sieci komputerowe.

Dzisiaj wirusy, robaki, konie trojańskie czy króliki osobom funkcjonującym w przestrzeni wirtualnej kojarzą się jednoznacznie z zagrożeniem, które należy zwalczać. Internet staje się zatem nieustannym polem rywalizacji między programistami piszącymi szkodliwe oprogramowanie, włamującymi się do systemów, wykradającymi dane a programistami likwidującymi powstałe w ten sposób straty i unieszkodliwiającyi zdradliwe aplikacje. Ponieważ szala zwycięstwa nie przechyla się (i pewnie nigdy nie przechyli) zdecydowanie w żadną ze stron, nikogo nie dziwi wszechobecne pytanie – czy zwykły użytkownik Internetu może czuć się w takich warunkach bezpiecznie?

Oddając w Państwa ręce niniejszy numer „Nowych Technologii”, próbujemy nie tyle odpowiedzieć na powyższe pytanie, ile pokazać między innymi skuteczne drogi bezpiecznego poruszania się po wirtualnym świecie. Ponieważ rzezone drogi wytyczane są często przez systemy Comarch, przybliżyliśmy te rozwiązania – z nadzieją, że pomogą Państwu uniknąć zastawianych w sieci pułapek. Bo choć Internet roi się od zagrażających użytkownikom zasadzek, od nas zależy, czy uciekniemy przed czyhającym na nas niebezpieczeństwem.

Zapraszamy i życzymy miłej lektury!

Redakcja Nowych Technologii

- 3. Od redakcji
- 4. Spis treści
- 6. Aktualności

## TEMAT NUMERU



### 10. Uwierzytelnianie i autoryzacja, czyli podstawa systemów webowych

Koniec dwudziestego wieku był czasem informatyzacji całego świata. Obecnie coraz więcej usług, w tym finansowych, dostępnych jest poprzez Internet. Zabezpieczenie ich, wiarygodne potwierdzenie tożsamości użytkownika oraz niezaprzeczalna autoryzacja transakcji stają się kluczowymi elementami każdego systemu webowego.

**Tomasz Śnieżyński**



### 14. Uwierzytelnienie i autoryzacja transakcji w dobie urządzeń mobilnych

Nie tak dawno możliwości technologiczne, jakie oferowały urządzenia mobilne, sprowadzały się do oglądania prostych stron internetowych z wykorzystaniem przeglądarek WAP. Obecnie rynek zmierza w kierunku wykorzystania przenośnych urządzeń, takich jak Smartphony, urządzenia PDA czy nawet zwykłe telefony komórkowe w coraz bardziej zaawansowanych biznesowych rozwiązaniach, m.in. bankowości elektronicznej czy systemach maklerskich.

**Maciej Wolański**



### 18. Zarządzanie dostępem i tożsamością. Korzyści dla użytkowników i administratorów

Odkąd powstała pierwsza aplikacja, z której mógł korzystać nie tylko jeden użytkownik, powstał problem w ich rozróżnianiu. Zadawano pytania, po co należałoby różnicować użytkowników, w jakich przypadkach, według jakich kryteriów, jak zarządzać uprawnieniami użytkowników. Wszystkie te pytania sprowadzały się tak naprawdę do jednego – w jaki sposób kontrolować dostęp do systemów teleinformatycznych i zarządzać nim.

**Tomasz Śnieżyński**



### 22. Niebezpieczeństwa płynące z sieci wewnętrznej korporacji

Na dzisiejszym rynku, a zwłaszcza na rynku związanym z nowoczesnymi technologiami, wartość informacji jest coraz większa w stosunku do zasobów materialnych posiadanych przez firmę i trend ten stale rośnie.

**Maciej Wolański**

## ROZWIĄZANIA I WDROŻENIA

### 26. Ubezpieczenia zdrowotne – nowe rozwiązania systemowe

Mimo zapewnionej publicznej służby zdrowia w każdym z krajów europejskich zainteresowanie prywatną opieką medyczną jest duże. Nie jest to tylko związane ze słabym systemem publicznym w niektórych krajach, który nie pokrywa 100 proc. zapotrzebowania obywateli na usługi medyczne i operacje, ale przede wszystkim wynika ze wzrastającej świadomości co do potrzeb ochrony własnego zdrowia i zdrowia bliskich.

**Marta Kardela-Trojanowska**

### 30. Higiena baz danych. Krótki zarys deduplikacji

Bazy i hurtownie danych rozrastają się obecnie w astronomicznym tempie. Duże instytucje dysponują bazami o wielkości rzędu dziesiątek milionów rekordów oraz setek kolumn. W tak dużym zbiorze danych nietrudno jest o błędne wpisy lub powtarzające się wiersze. Aby zapewnić swoim klientom jak najlepszą jakość obsługi oraz zachować jak najwyższą wydajność baz danych, okresowe czyszczenie przechowywanych informacji powoli staje się koniecznością.

**Bartłomiej Kozakowski**

### 36. Ocean jest Agile. Ocean w Administracji Publicznej

Ocean to nieustanny rozwój. Rozwiązanie średniego kalibru w ciągu roku przерodziło się w rodzinę produktów, których wspólnym celem jest realizacja głównego założenia: Adresacja Biznesowych Potrzeb Klienta, w skrócie – Agile.

**Julia Domańska**

### 40. OCEAN możliwości. Wdrożyliśmy OCEAN w Urzędzie Miasta Ciechanów

Zadanie: Dostawa sprzętu komputerowego i oprogramowania oraz świadczenie usług w ramach projektu „Budowa i wdrożenie publicznego, interaktywnego systemu usług administracji samorządowej e-Urząd (Etap I).

**Michał Grabowski**

### 42. Rozwiązania na miarę nagród

Przyznawane regularnie nagrody i wyróżnienia na bieżąco wyznaczają nowe trendy w branży IT oraz stanowią potwierdzenie sprawdzonych i efektywnych systemów.

**Maria Sulisz**

## TRENDY I STRATEGIE

### 45. ITIL – koszt czy wartość dodana?

Do niedawna outsourcing systemów informatycznych odbywał się na zasadzie negocjacji kontraktu pomiędzy stronami. Nie występowały żadne zalecenia dotyczące sposobu obsługi podmiotu outsourcowanego. Stan taki powodował wiele konfliktów i nieporozumień na osi przedsiębiorstwo – firma outsourcingowa.

**Andrzej Nowacki**

### 48. Wirtualizacja. Czas na przyszłość

Hasło „wirtualizacja zasobów IT” zdobywa i podbija dzisiaj cały świat. Szaleństwo wirtualizacji jakiś czas temu trafiło również do Polski i zagościło już na dobre w rodzimych serwerowniach.

**Miłosz Brzozowski**

### 54. Software as a Service (SaaS). Nowe możliwości Comarch Data Center

Model SaaS, zdobywający coraz większą popularność na rynku rozwiązań IT, zachęca do zagłębienia się w jego istotę potencjalnymi możliwościami obniżenia kosztów TCO, podniesienia dostępności rozwiązania i innych korzyści wynikających z jego charakterystyki. Jak przedstawia się to z perspektywy Comarch Data Center?

**Jakub Pysz**

### 57. Dostęp satelitarny – wczoraj, dziś i jutro

Historia telekomunikacji satelitarnej zaczęła się w październiku 1945 r. Wówczas to w brytyjskim magazynie „Wireless World” były oficer Królewskich Sił Powietrznych Arthur Charles Clarke opublikował artykuł naukowy pt. „Extraterrestrial Relays”, w którym zawarł ideę wykorzystania satelitów umieszczonych na orbitach geostacjonarnych do stworzenia światowej sieci łączności.

**Michał Szybalski**

## Comarch odnotował dwudziestoprocentowy wzrost sprzedaży usług i oprogramowania własnego

W pierwszym półroczu 2008 roku przychody ze sprzedaży Comarch wzrosły w porównaniu z pierwszym półroczem 2007 o 1,7 procent do 275,1 miliona złotych. Wzrost sprzedaży usług i oprogramowania własnego firmy wyniósł łącznie 32,6 miliona złotych, czyli 20,5 procent.

W skali pierwszego półroczu 2008 roku, po wyeliminowaniu zdarzeń jednorazowych, Comarch osiągnął dobre wyniki finansowe, porównywalne do osiągniętych w pierwszym półroczu 2007 roku. Uwagę zwraca

zwłaszcza zdecydowany wzrost przychodów ze sprzedaży produktów i usług własnych Comarch (wzrost o 32,6 miliona złotych), który pozwolił zniwelować efekt znaczącego wzrostu wynagrodzeń odnotowanego w roku 2007 i mającego wpływ na poziom kosztów w pierwszych dwóch kwartałach 2008 roku.

Skorygowana rentowność operacyjna wyniosła w pierwszych dwóch kwartałach 7,8 procent i osiągnęła poziom wyższy od odnotowanego rok wcześniej, to jest 7,2 procent.

Skorygowana rentowność netto utrzymała się na poziomie 7,0 procent, porównywalnym do 6,9 procent rok wcześniej.

Portfel zamówień na rok bieżący wynosił na koniec lipca 2008 roku 489,9 miliona złotych i był wyższy o 0,6 procent niż w analogicznym okresie w 2007 roku, przy czym wzrost zamówień na produkty i usługi własne Comarch wyniósł 20,6 procent.

– *Znaczący wzrost portfela zamówień na produkty i usługi własne*

*w porównaniu z analogicznym okresem ubiegłego roku potwierdza dalsze możliwości dynamicznego rozwoju Comarch w kolejnych okresach. Zwiększenie rentowności operacyjnej poprzez sprzedaż własnych rozwiązań pozostaje jednym z najważniejszych priorytetów firmy w bieżącym roku i kolejnych latach* – komentuje Janusz Filipiak, Prezes Comarch SA.

Udział kontraktów zagranicznych w portfelu zamówień pozostaje na stabilnym poziomie 20,5 procent, mimo bardzo mocnej złotówki.

## Prestiżowa nagroda dla Comarch ALTUM

Comarch ALTUM po raz kolejny został doceniony przez międzynarodowe jury i znalazł się wśród laureatów konkursu „Microsoft Partner Program Awards 2008” jako zwycięzca kategorii „ISV / Software Solutions”. Nagrody zostaną wręczone podczas konferencji dla partnerów Microsoft – Worldwide Partner Conference 2008, organizowanej w dniach 7-10 lipca 2008 w Houston w Teksasie.

Celem konkursu „Microsoft Partner Program Awards” – organizowanego corocznie dla producentów oprogramowania, a zarazem partnerów giganta z Silicon Valley – jest uhonorowanie tych firm, które dostarczają najbardziej innowacyjne rozwiązania tworzone na bazie narzędzi Microsoft. Zwycięzców 23 konkur-

sowych kategorii wyłoniono z grona 47 000 firm z całego świata. Systemy oceniano pod względem dopasowania do potrzeb i oczekiwań klientów, rozwiązania ich problemów biznesowych oraz innowacyjności.

– *Bardzo cieszy nas nagroda ISV / Software Solutions Partner of the Year, którą Microsoft przyznał Comarch SA za produkt Comarch ALTUM na światowej konwencji w Houston w USA w lipcu tego roku. Comarch SA ponosi bardzo duże nakłady inwestycyjne na prace badawczo-rozwojowe, starając się być w światowej czołówce producentów oprogramowania dla przedsiębiorstw. Przykładem pozytywnego wyniku tych prac jest system Comarch ALTUM, opracowany w najnowszych narzędziach Micro-*

*soft. Umożliwia on w przystępnej cenie wdrożenie w firmach małych i średniej wielkości funkcjonalności takich, jak konfigurowalny Work Flow i Business Intelligence, które do tej pory były dostępne wyłącznie dla dużych korporacji. Ergonomia i orientacja procesowa systemu są wynikiem ponad piętnastu lat doświadczeń Comarch w produkcji systemów ERP dla przedsiębiorstw. Przygotowanie produktu innowacyjnego na poziomie światowym było możliwe dzięki wieloletniej i głębokiej współpracy obu firm. W ramach partnerstwa strategicznego inżynierowie Comarch mieli stały dostęp do najnowszych, przedkomercyjnych technologii Microsoft opracowywanych w laboratoriach w Redmond – powie-*

dział profesor Janusz Filipiak, Prezes Zarządu Comarch SA.

Nagroda od Microsoft to już trzeci międzynarodowy sukces nowego systemu ERP firmy Comarch. Zaledwie kilka tygodni po swojej światowej premierze w marcu br. Comarch ALTUM otrzymał wyróżnienie „Innovations Produkt” w konkursie na najbardziej nowatorski system ERP organizowanym w czasie targów CeBIT. Prestiżową nagrodę oraz tytuł „Best Solution Provider Product / Solution” przyznano Comarch ALTUM również w czasie konferencji Gartnera „IT ChannelVision Europe 2008”, podczas której najnowsze rozwiązanie Comarch zdobyło uznanie jury i większości menedżerów z blisko 200 firm branży IT z całego świata.

## Zakończenie wdrożenia Comarch Contact Center w Invest Banku

Sukcesem zakończyło się wdrożenie systemu Comarch Contact Center. Celem projektu było stworzenie infrastruktury kompleksowego rozwiązania contact center wraz z systemem CRM, wspierającym działania biznesowe realizowane przez pioniera obsługi klienta w InvestBanku.

– *Integracja platformy Contact Center firmy Avaya, światowego lidera w tej dziedzinie, z aplikacją biznesową Comarch CRM była odpowiedzią na potrzeby klienta. Obserwujemy znaczne zwiększenie zainteresowania tego rodzaju rozwiązaniami, gdyż samo rozwiązanie*

*call czy contact center to dzisiaj za mało. Firmy równie mocno potrzebują całej warstwy analityczno-biznesowej dla realizacji swoich zadań operacyjnych oraz budowania przewagi konkurencyjnej. Nasze rozwiązanie dzięki rozbudowanej funkcjonalności, elastyczności oraz wysokiej*

*jakości komponentów spełnia wymagania klientów* – mówi Marcin Pepaś, Kierownik Subcentrum Rozwiązań Sieciowych i Telekomunikacyjnych, Centrum Konsultingu Infrastruktury IT Sektora Usług, Comarch SA.

## Comarch ma kontrakt z PEWIK Gdynia

Comarch podpisał umowę na dostawę i wdrożenie systemu do zarządzania przedsiębiorstwem w PEWIK Gdynia (Przedsiębiorstwo Wodociągów i Kanalizacji Spółka z o.o.). Kwota kontraktu to 1 450 580 PLN brutto.

Projekt obejmuje wszystkie obszary wsparcia informatycznego. Począwszy od finansów i księgowości, przez kadry i płace, aż po billing oraz biuro obsługi klienta. Ponadto obszar obsługi technicznej będzie zintegrowany z funkcjonującym obecnie systemem GIS. Projekt realizowany jest wspólnie z partnerem Comarch – firmą MEGABIT, która jest odpowiedzialna za moduł Remonty i Obsługa Techniczna Sieci ( ROT).

– Wdrożenie w Przedsiębiorstwie Wodociągów i Kanalizacji w Gdyni

to kolejny kontrakt w przedsiębiorstwach wodociągowych realizowany przez Comarch. System usprawni pracę w obszarach związanych z obsługą klienta oraz jako zintegrowane rozwiązanie ERP pozwoli na szybszy dostęp do informacji o stanie przedsiębiorstwa – wyjaśnia Tomasz Nakonieczny, Dyrektor gdańskiego oddziału Comarch.

– Obecnie używany w PEWIK Gdynia sp. z o.o. system, dostarczony przez firmę Kom-Pakt, w większości przypadków oceniany był jako przestarzały i niespełniający wymogów stawianych nowoczesnym systemom tego typu – mówi Cecylia Pietraszewska, kierownik dz. Informatyki PEWIK Gdynia. – Pociągało to za sobą konsekwencje w postaci częstych mody-

fikacji, mających na celu wyeliminowanie braku funkcjonalności lub dostosowywanie do wymogów przepisów i innych wymagań zarówno wewnętrznych, jak i zewnętrznych. Równocześnie wykorzystywane w nim rozwiązania technologiczno-informatyczne nie spełniały wymogów stawianych obecnie rozwiązaniom IT. Współpraca z firmą Kom-Pakt rozpoczęta została wiele lat temu. W 2003 r. nastąpiła rozbudowa systemu o kolejne moduły oraz jeden nowy moduł związany z obiegiem dokumentów. Decyzja o zmianie systemu podjęta została na początku 2007r. Od tego czasu rozpoczął się proces wyboru dostawcy oraz przede wszystkim określenie wymagań, warunków technicznych i funkcjonalnych, które

zostały postawione przed nowym systemem, opartych na oczekiwaniach poszczególnych komórek organizacyjnych PEWIK Gdynia sp. z o.o. Po fazie negocjacji z zaproszonymi do nich uczestnikami, uwzględnieniu cen oraz stopnia spełniania określonych warunków technicznych, wyłoniony został zwycięzca, a zarazem firma, która przeprowadzi wdrożenie nowego Zintegrowanego Systemu Informatycznego w PEWIK Gdynia sp. z o.o., tj. Comarch. Po wdrożeniu spodziewana jest poprawa w wielu obszarach funkcjonowania przedsiębiorstwa, a współpraca z firmą, której system ERP działa m.in. w Gdańskim PEC, OPEC Gdynia, Elbląskim PEC, PEC Malbork oraz Sydkraft EC Słupsk, daje gwarancję na końcowy sukces.

## Comarch wdroży system ECOD Dystrybucja w Stella Pack SA

Comarch SA i Stella Pack SA zawarły umowę na wdrożenie i serwis systemu ECOD Dystrybucja w modelu SaaS (Software as a Service). To już trzeci system autorstwa Comarch po ECOD Operator i ECOD Agent wdrażany w firmie Stella Pack.

– SaaS polega na udostępnieniu całego systemu informatycznego w formie usługi biznesowej. Klient nie płaci za aplikację, sprzęt, licencje firm trzecich czy usługi wdrożeniowe. Płaci miesięczną opłatę za otrzymanie konkretnych usług biznesowych zgodnie z ustalonym SLA. Ten typ kupowania informatyki cie-

szysię na rynku coraz większą popularnością. Comarch ma już prawie 8-letnie doświadczenie w realizacji projektów w tym modelu. Zdecydowanie ponad 50 proc. przychodów uzyskiwanych przez nas na rynku Retail&FMCG pochodzi ze sprzedaży naszych usług i licencji w modelu SaaS. Dodatkowo cieszy fakt, że obecnie w modelu SaaS realizujemy liczne projekty za granicą, między innymi dla klientów z Niemiec, Francji, Hiszpanii, Rosji czy Ukrainy – tłumaczy Marcin Warwas, Wiceprezes Comarch SA odpowiedzialny za Sektor Usługi.

– ECOD Dystrybucja to usługa skierowana do firm posługujących się zewnętrzną siecią dystrybucji. Pozwala na regularne i szybkie uzyskiwanie aktualnych informacji o sprzedaży z sieci dystrybucyjnej. Umożliwia ona także optymalizację produkcji i stanów magazynowych zarówno po stronie producenta, jak i dystrybutora. ECOD Dystrybucja usprawnia również procesy logistyczne oraz obniża koszty magazynowania – mówi Jarosław Gaik, Kierownik Działu IT Stella Pack SA.

ECOD Dystrybucja jest usługą umożliwiającą firmom współpracują-

cym z zewnętrzną siecią dystrybucji, przez którą realizowana jest sprzedaż do sklepów detalicznych, na pozyskiwanie i raportowanie codziennie aktualnych informacji biznesowych (np. o odsprzedaży albo aktualnych stanach magazynowych).

Stella Pack SA to jeden z wiodących producentów worków na śmieci oraz lider rynku produktów z mikrofibry oraz rękawic w Polsce. W swojej ofercie posiada też szerokie portfolio artykułów opakowaniowych, takich jak: produkty do pieczenia, folie aluminiowe, woreczki, torebki itp.

## Comarch po raz czwarty z rzędu największym polskim integratorem systemów IT

Comarch zdobył tytuł największego polskiego eksportera IT w 2007 roku oraz po raz czwarty z rzędu został uznany za największego polskiego integratora systemów IT w prestiżowym rankingu Computerworld TOP 200. Przedsiębiorstwo zostało także liderem wśród firm osiągają-

cych przychody z obsługi sektora handel hurtowy.

– Szczególnie cieszy nas otrzymana w tym roku nagroda dla największego polskiego eksportera IT. Dowodzi ona właściwie obranej strategii rozwoju biznesowego i sukcesów na zagranicznych rynkach, jakie odnosi Comarch

oraz wyprodukowane w firmie innowacyjne produkty IT. Dołożyliśmy wszelkich starań, aby rok 2008 zaowocował nagrodami w następnej edycji rankingu Computerworld TOP 200 – mówi prof. Janusz Filipiak, Prezes Comarch.

Ranking Computerworld TOP 200 poświęcony polskiemu rynkowi IT

ukazuje się od 1995 roku. Raport zawiera przetworzone dane finansowe największych polskich firm informatycznych i telekomunikacyjnych oraz rankingi firm IT świadczących usługi i oferujących szkolenia, a także producentów sprzętu, dystrybutorów oraz integratorów.

## Comarch w prestiżowym gronie Symbian Partner Program

Comarch ogłosił przystąpienie do programu partnerskiego – Symbian Partner Program. Firma w ramach wsparcia rosnącego rynku telefonów komórkowych z systemem operacyjnym Symbian oferuje specjalistyczną wiedzę oraz bogate portfolio profesjonalnych usług IT dla środowiska Symbian. Symbian Limited rozwija i licencjonuje Symbian OS – wiodącą platformę na rynku systemów operacyjnych dla telefonów komórkowych. Ten system operacyjny został zaakceptowany przez czołowych producentów urządzeń mobilnych, czego rezultatem jest

dostarczenie ponad 188 milionów urządzeń mobilnych z systemem Symbian OS do ponad 250 największych operatorów telefonii komórkowych na całym świecie.

Comarch, który może się poszczycić długą historią współpracy z największymi producentami urządzeń mobilnych, podjął strategiczną decyzję, by wspierać platformę Symbian OS. Taki rodzaj współpracy skutkuje poszerzeniem możliwości rozwoju obu firm i nawiązaniem nowych kontaktów biznesowych z licznymi partnerami.

– *Coraz więcej firm ma innowacyjne pomysły na rozwój aplikacji mobilnych,*

*ale nie posiada odpowiednich umiejętności albo mocy produkcyjnych, aby je zrealizować. Wraz z przystąpieniem Comarch do Programu Partnerskiego, w którego skład wchodzi zarówno Symbian, jak i rosnąca sieć partnerów, producentów telefonów komórkowych i operatorów, firmy te otrzymają pomoc, której potrzebują, by urzeczywistniać swoje pomysły i tworzyć nowoczesne aplikacje dla Symbian OS* – mówi Jerry Panagrossi, wiceprezes i dyrektor Generalny North American Operations, Symbian.

– *W związku z coraz większą ekspansją telefonów z Symbian OS na*

*masowym rynku, Comarch zapewnia, że będzie kontynuował profesjonalny rozwój i tworzenie aplikacji dla Symbian OS. Nasza bliska współpraca z największymi producentami urządzeń mobilnych i wiodącymi operatorami telefonii komórkowych na rynku daje nam unikalną szansę wywarcia wpływu na akceptację smartfonów z systemem Symbian zarówno przez klientów indywidualnych, jak i biznesowych* – mówi Paweł Bieryt, dyrektor Działu Professional Services w Sektorze Telekomunikacji, Comarch SA.

## Comarch wdroży system lojalnościowy w firmie Bayer

Comarch podpisał z firmą Bayer umowę na wdrożenie Comarch Loyalty Management, jednego z najbardziej zaawansowanych technologicznie i funkcjonalnie systemów do obsługi programów lojalnościowych na świecie. Rozwiązanie ma być wdrożone na potrzeby Bayer CropScience.

System firmy Comarch zapewni wsparcie realizacji programu lojalnościowego w branży ochrony roślin. Program lojalnościowy będzie realizowany przy współpracy z siecią 140 partnerów handlowych w całej Polsce.

– *Wdrażane rozwiązanie będzie obsługiwać jedną z kluczowych dla firmy*

*platform współpracy z klientami – program lojalnościowy prowadzony z dużym sukcesem od 5 lat. Wykorzystanie systemu Comarch Loyalty Management pozwoli nam na efektywniejszą segmentację rynku oraz pogłębienie wiedzy na temat zachowań zakupowych klientów. Równocześnie będzie to jedno z najnowocześniejszych narzędzi wykorzystanych w branży ochrony roślin* – mówi Urszula Filipecka, Szef Serwisu Marketingowego, Bayer CropScience.

– *Comarch Loyalty Management (CLM) gwarantuje możliwość centralnego zarządzania programem lojal-*

*nościowym w Bayer CropScience. Będzie odpowiedzialny za przetwarzanie wszystkich danych w systemie – począwszy od budowy schematów lojalnościowych, aż po poszczególne transakcje. W ramach tworzonych programów lojalnościowych wydawane będą karty będące jedynie identyfikatorem klienta. Informacje o klientach będą przechowywane w Systemie Centralnym i udostępniane w czasie rzeczywistym w lokalizacjach* – wyjaśnia Marcin Warwas, wiceprezes Comarch odpowiedzialny za sektor Usługi.

System będzie umożliwiał również generowanie dodatkowych

komunikatów marketingowych po każdej transakcji lojalnościowej, udostępnianych na wyświetlaczu kasy lub drukowanych na paragonie sprzedaży. System CLM zostanie zintegrowany z systemem CRM Bayer, a w przyszłości zakładana jest również ścisła integracja systemu z systemami kasowymi Partnerów Bayer CropScience. Całość systemu będzie hostowana w Comarch Data Center, co zapewnia wykorzystanie najwyższej klasy platformy sprzętowej, a także przetwarzanie transakcji w czasie rzeczywistym.

## Comarch firmą przyjazną środowisku

Comarch włączył się w ogólnopolską oraz międzynarodową akcję Święto Drzewa, której inauguracja odbyła się 10 października 2008 r. w Warszawie. Udział w akcji to jeden z elementów długofalowego projektu Eko Comarch.

W 2008 roku Comarch po raz pierwszy włączył się w program Święto Drzewa, w nadziei, że współpraca z Klubem Gaja przyniesie wymierne korzyści dla środowiska.

– *Coraz więcej firm wpisuje się w nowy, zrównoważony kierunek rozwoju, w którym dbałość o środowisko naturalne staje się jednym z priorytetów na stałe umieszczonych w misji firmy* – komentuje Aneta Malec, Kierownik Wsparcia Sprzedaży, Comarch SA. – *Podobnie jest w przypadku Comarch, dlatego rozpoczęliśmy projekt ekologiczny Eko Comarch. Jednym z pierwszych działań, jakie podjęliśmy, była rezygnacja*

*z materiałów papierowych podczas cyklu konferencji* – dodaje.

Comarch bierze udział w wielu działaniach ekologicznych, do których należy m.in. ograniczenie materiałów papierowych, rezygnacja z jednorazowych reklamówek na rzecz toreb ekologicznych, wymiana drukowanych podręczników na instrukcję w formie płyty CD. Równocześnie Comarch szerzy świadomość ekologiczną wewnątrz firmy – w tym celu została przeprowadzona akcja

„Kubek za kubek”, która doprowadziła do wyeliminowania plastikowych kubków z firmy. W zamian każdy pracownik otrzymał ceramiczny kubek z logo akcji.

Projekt Eko Comarch jest procesem długofalowym o nieocenionych efektach dla przyszłych pokoleń, dlatego firma jest zdecydowana na promowanie ekologicznych zachowań oraz na rozwijanie projektu.

Szczegóły akcji mogą Państwo znaleźć na stronie [www.ekocomarch.pl](http://www.ekocomarch.pl)

## Comarch w WĘGLOKOKS SA

Comarch podpisał umowę z firmą WĘGLOKOKS SA na dostawę i wdrożenie Zintegrowanego Systemu Informatycznego. Wdrożenie systemu w WĘGLOKOKS SA to pierwszy tak duży projekt w tej branży realizowany w Polsce.

– Podpisanie umowy z Comarch stanowiło zwieńczenie wielomiesięcznego procesu mającego na celu wyłonienie wykonawcy systemu. Wyniki postępowania przetargowego i rokowań pozwalają wyrazić przekonanie, iż oferowane przez Comarch rozwiązania spełnią oczekiwania WĘGLOKOKS SA. Jesteśmy zadowoleni z dokonanego wyboru i liczymy na pełną i sprawną realizację procesu wdrożenia, jak i funk-

cjonowania zaproponowanego systemu. Uważam, iż gwarancją spełnienia naszych oczekiwań jest solidność i wysoka pozycja firmy Comarch na rynku – mówi Piotr Kozioł, Prezes Zarządu WĘGLOKOKS SA.

W ramach umowy Comarch dostarczy i wdroży oprogramowanie Oracle e-Business Suite oraz niezbędną infrastrukturę sprzętową. Wdrożenie obejmie wszystkie obszary działalności WĘGLOKOKS SA, a mianowicie: finanse, controlling, logistykę, zakupy, sprzedaż, kadry, płace, CRM, workflow, hurtownię danych oraz BI.

– Wdrożenie w WĘGLOKOKS SA to jedno z większych wdrożeń realizowanych przez Comarch w branży

węglowej. Globalny wzrost zapotrzebowania na węgiel sprawia, że przedsiębiorstwa te będą w najbliższym czasie rozwijały swoje moce wydobywcze i wdrażały wspierające je nowoczesne rozwiązania informatyczne. System, który dostarczy Comarch, będzie obsługiwał większość procesów biznesowych, pozwoli znacząco zwiększyć efektywność pracy oraz obniżyć koszty funkcjonowania firmy – mówi Paweł Prokop, Wiceprezes Zarządu Comarch odpowiedzialny za sektor publiczny.

Wdrożenie systemu ułatwi dostęp do informacji z różnych obszarów oraz przede wszystkim pozwoli na dokładną analizę kosztów i przy-

chodów spółki. Elektroniczny obieg dokumentów poprawi kontrolę nad procesami zachodzącymi w bieżącej działalności firmy. Część wdrożenia będzie obejmowała obszary, które teraz nie są z informatyzowane w WĘGLOKOKS SA.

– Wybór systemu Oracle E-Business Suite jest dowodem bardzo szerokiej funkcjonalności aplikacji Oracle i racjonalności kosztów ich implementacji. Godna podkreślenia jest także znakomita, wręcz podręcznikowa współpraca z firmą Comarch, będącą obecnie jednym z największych i najbardziej kompetentnych partnerów aplikacyjnych Oracle w Polsce – mówi Marek Wdowicz, Dyktor sprzedaży aplikacji w Oracle Polska.

## Comarch Debt Management w Allianz Banku

Comarch zawarł z Allianz Bankiem umowę na wdrożenie systemu do windykacji wierzytelności Comarch Debt Management. System ten od czterech lat z powodzeniem funkcjonuje w spółkach ubezpieczeniowych grupy Allianz.

Projekt wdrożeniowy obejmuje pełną funkcjonalność systemu oraz wysoki stopień automatyzacji

działań, co pozwoli na szybką i skuteczną realizację procesów monitoringu i windykacji należności bankowych.

– System Comarch Debt Management łączy w sobie doświadczenie Comarch zdobyte w zakresie informatycznego wsparcia procesów windykacji, wiedzę biznesową w sektorze bankowości oraz znajomość

specyfiki grupy Allianz, z którą dostawca systemu współpracuje już od kilku lat – mówi Dyktor Departamentu Windykacji Allianz Banku Adrian Babij.

– Comarch Debt Management to uniwersalny system zarządzania wierzytelnościami kierowany do różnorodnych firm i instytucji, które w ramach swojej działalności

prowadzą prewindykację, windykację przedsądową oraz windykację twardą (postępowanie sądowe oraz egzekucyjne), a także zlecają sprawy windykacyjne podmiotom zewnętrznym. Comarch Debt Management dobrze się sprawdza również jako podstawowy system dla spółek windykacyjnych – dodaje Maciej Ślósarczyk, Product Manager Comarch.

## Comarch Asset Management w OTP Capital

Comarch zawarł z ukraińską firmą AMC OTP Capital umowę na wdrożenie systemu do zarządzania aktywami Comarch Asset Management. AMC OTP Capital należy do międzynarodowej grupy finansowej OTP Group. Obecnie firma OTP Capital zarządza aktywami trzech otwartych funduszy inwestycyjnych.

Projekt wdrożenia i automatyzacji obejmuje wszystkie kluczowe obszary działalności OTP w zakresie sprzedaży, obsługi, księgowości i zarządzania funduszami inwestycyjnymi oraz emerytalnymi. W ramach

projektu realizowana jest m.in. integracja z platformą transakcyjną PFTS oraz moduł sprawozdawczy do organów nadzoru. Dostarczany jest również moduł odpowiedzialny za obsługę klientów funduszy i operacji na tytułach uczestnictwa w funduszach.

– System Comarch łączy w sobie doświadczenia zdobyte na rynku Unii Europejskiej i Rosji, oferując jednocześnie funkcjonalność specyficzną dla regulacji Ukrainy. Pozwoli nam to sprawnie działać dziś i jednocześnie być przygotowanym na wyzwania

przyszłości – mówi Maryna Pavlivna Mendzebrovska, Dyktor Generalny AMC OTP Capital.

Dzięki bogatemu doświadczeniu nabytemu na rynku polskim oraz rosyjskim Comarch mógł zaoferować w pełni dojrzały produkt, który wspomaga zarządzanie aktywami w kilkudziesięciu firmach ubezpieczeniowych, asset management oraz funduszach emerytalnych w Polsce i Rosji.

– AMC OTP Capital to czwarta ukraińska firma zarządzająca aktywami, która w okresie ostatnich

12 miesięcy zdecydowała się na wybór rozwiązania Comarch Asset Management. Dotychczas były to wiodące firmy z kapitałem ukraińskim – OTP Capital należy do grupy finansowej o znaczeniu międzynarodowym. Cieszymy się z pozytywnej oceny wystawionej naszemu rozwiązaniu w Budapeszcie, gdzie znajduje się główne biuro OTP Group – mówi Grzegorz Prosovicz, Dyktor w Centrum Konsultingu Rynków Kapitałowych Sektora Finansów i Ubezpieczeń Comarch.

# Uwierzytelnianie i autoryzacja

CZYLI PODSTAWA SYSTEMÓW WEBOWYCH



Koniec dwudziestego wieku był czasem informatyzacji całego świata. Obecnie coraz więcej usług, w tym finansowych, dostępnych jest poprzez Internet. Zabezpieczenie ich, wiarygodne potwierdzenie tożsamości użytkownika oraz niezaprzeczalna autoryzacja transakcji stają się kluczowymi elementami każdego systemu webowego.



**W NINIEJSZYM** artykule zostanie dokonany przegląd metod uwierzytelnienia i autoryzacji. Zostaną wskazane ich wady i zalety. Moim celem jest uzmysłowienie zagrożenia lub pozornego bezpieczeństwa i przekonanie, iż warto inwestować w nowoczesne metody uwierzytelniania i autoryzacji. Pamiętajmy również, że uwierzytelnienie i autoryzacja to nie wszystko. Do bezpieczeństwa należy podchodzić w sposób całościowy i zaprojektować odpowiednie mechanizmy adekwatne dla danych zagrożeń, grup użytkowników czy typów transakcji do potwierdzenia. Nie wszyscy muszą stosować mechanizmy najsilniejsze i najbardziej zaawansowane technicznie. Ale to już powinna definiować polityka bezpieczeństwa danej organizacji.

## Uwierzytelnienie i autoryzacja wczoraj i dzisiaj

### Hasła statyczne

Najpopularniejszą metodą uwierzytelnienia się, czyli potwierdzenia swojej tożsamości, jest wykorzystanie statycznego ciągu znaków, czyli krótko mówiąc hasła. Jej bezpieczeństwo zależy jednak w dużej mierze od użytkownika, od tego, czy postępuje zgodnie z pewnymi zasadami. Hasła statyczne są jak bielizna osobista:

- ▶ należy je często zmieniać,
- ▶ nie współdzielić z przyjaciółmi,
- ▶ im są dłuższe, tym są lepsze,
- ▶ nie należy pozostawiać ich na widoku,
- ▶ powinny być tajemnicze.

Uwierzytelnienie hasłem powinno być zatem wspomagane zawsze przez mechanizmy, które zadbają o odpowiednią jakość hasła, będą wymuszać jego częstą zmianę, ale na to, czy użytkownik będzie je przechowywał jedynie w swojej pamięci, czy zapisze na przysłowiowej żółtej karteczce i przyklei pod podkładką myszki – już nie mamy wpływu. Należy pamiętać jeszcze o jednym czynniku całej układanki, a mianowicie o osobach, które wszelkimi możliwymi metodami chcą zdobyć nasze hasło, kompromitując je. Stosują one najczęściej metody socjotechniki, phishingu lub złośliwe oprogramowanie. (W ostatniej części artykułu przybliżymy nieco te pojęcia.) Złośliwe oprogramowanie może słuchać transmisji pomiędzy użytkownikiem a serwerem webowym. Jeżeli transmisja nie jest szyfrowana, hasło jest wystawione hackerowi niemalże na tacy. Samo jednak szyfrowanie transmisji już dzisiaj nie wystar-

cza i aby uchronić się przed takimi atakami jak Man-In-The-Middle, szyfrowanie powinno być wcześniej obustronnie uwierzytelnione. Złośliwe oprogramowanie może w końcu być zainstalowane na stacji końcowej nieświadomego użytkownika i tam śledzić każdy znak wprowadzany przez użytkownika z klawiatury bądź bezpośrednio przechwytywać hasła z okienek. W pierwszym przypadku można stosować softwarowe klawiaturki, aby nie wprowadzać znaków z fizycznej klawiatury, lecz wskazywać je na ekranie myszką. Sama klawiatura to jednak zabezpieczenie niewystarczające. Hacker wciąż może zczytywać położenie kursora myszki podczas wpisywania hasła, a następnie współrzędne zamienić na znaki. Klawiaturka softwarowa, aby wносиła żądany poziom bezpieczeństwa, powinna za każdym razem pojawiać się w innym miejscu ekranu oraz za każdym razem znaki powinny być rozmieszczone na niej w innej kolejności. Czy jest to wygodne – zdecydowanie nie.

Jak pokazano powyżej, aby posługiwanie się hasłem statycznym było bezpieczne, system powinien być wyposażony w szereg dodatkowych zabezpieczeń, a i tak nie od wszystkiego te zabezpieczenia są w stanie uchronić. Jeżeli użytkownik zapisze sobie swoje hasło na karteczce, nic z tym nie zrobimy. Należy zwrócić uwagę jeszcze na fakt, iż raz zdobyte hasło statyczne może być wielokrotnie używane przez hakera aż do momentu, gdy użytkownik się zorientuje, że coś jest nie tak.

Hasła statyczne mogą być również odgadywane przez zastosowanie ataków typu brute force. Aby utrudnić ten proceder, wprowadza się silne polityki haseł wymuszające odpowiednią ich jakość. Można również wprowadzić hasła maskowalne. Polegają one na tym, iż użytkownik definiuje długie hasło, które powinno się składać co najmniej z kilkunastu znaków, natomiast podczas logowania podaje on jedynie kilka znaków z całego hasła wskazanych przez system, przez daną maskę. Podsluchanie takiego hasła skutkuje tym, iż haker jednorazowo nie może zdobyć wszystkich znaków hasła, a co za tym idzie, więcej czasu musi poświęcić na taki atak, co może go w ostateczności zniechęcić. Ale czy hasła maskowalne są bezpieczne?

W bardzo prosty sposób wylicza się siłę haseł maskowalnych i prawdopodobieństwo skutecznego ich odgadnięcia, co może być tematem kolejnego artykułu. Aby utrudnić kompromitację haseł, dodatkowo można wprowadzić blokadę konta po x nieudanych próbach uwierzytelnienia. Na pewno w porównaniu do zwykłych haseł hasła masko-

walne podnoszą bezpieczeństwo. Na pewno również zwiększają frustrację użytkowników podczas wprowadzania takiego hasła. Haseł statycznych – czy to w wydaniu standardowym, czy w maskowalnym – więc nie polecamy i jednoznacznie kwalifikujemy tę metodę jako, nie używając silnych słów, nienowoczesną.

### Hasła jednorazowe

Skoro hasła statyczne po przechwyceniu stają się narzędziem doskonałym w rękę hakera, zaczęto wprowadzać mechanizmy umożliwiające generację haseł jednorazowych i wykorzystywanie ich do uwierzytelnienia się bądź autoryzacji. Przechwycenie takiego hasła nie prowadzi do niczego, ponieważ jest ono w swojej istocie jednokrotnego wykorzystania, dlatego pozostaje dla hakera bezużyteczne.

Z reguły hasła takie generowane są przez urządzenia zewnętrzne, przypominające swoim wyglądem breloki, karty kredytowe bądź małe kalkulatorki. Często, lecz niekoniecznie, hasło takie jest powiązane z PIN-em (ang. Personal Identification Number), czyli dodatkowym hasłem znanym użytkownikowi.

Zwróćmy uwagę, iż urządzenia takie wprowadzają dwuskładnikowe uwierzytelnienie: za pomocą czegoś, co użytkownik wie (pin), oraz za pomocą czegoś, co użytkownik posiada. Potencjalny haker, aby dostać się do systemu, musi po pierwsze zdobyć takie urządzenie, które powiązane jest jednoznacznie z użytkownikiem, oraz zdobyć dodatkowy PIN. Bezpieczeństwo w przypadku wykorzystywania haseł jednorazowych drastycznie nam rośnie. Rozwiązania takie, jak Comarch MobileID, umożliwiają generację haseł jednorazowych nawet na urządzeniach mobilnych, takich jak telefony czy smartfony (szerzej o Comarch MobileID w kolejnym artykule). Świetnie spisują się do uwierzytelnienia użytkowników, a niektórzy stosują je nawet do autoryzacji transakcji. Zatrzymajmy się na chwilę przy drugim zastosowaniu. Generator jest powiązany z użytkownikiem w systemie informatycznym, zatem użytkownik posługujący się nim może potwierdzić, iż faktycznie to on chce dokonać autoryzacji danej operacji. Jednak generatory takie w żaden sposób nie wiążą w tworzonych przez siebie hasłach informacji o transakcji, co staje się kluczowe w dzisiejszym świecie, aby rzetelnie zabezpieczyć operacje finansowe.

Hasła jednorazowe mogą być wysyłane na telefony komórkowe użytkowników w formie krótkiej wiadomości tekstowej (SMS). W przypadku wykorzystania ich do autoryzacji transakcji, SMS-y takie



niosą również w sobie z reguły podstawowe informacje o danej transakcji. Przez system teleinformatyczny informacje o transakcji mogą być również zaszyte w generowanym hasle jednorazowym. Sprawdzenie jednak, czy następuje autoryzacja transakcji faktycznie spodziewanej, czy też podmienionej przez hakera, uzależnione jest od tego, czy odbiorca SMS-a dokładnie przeczyta informacje w nim zawarte. Niestety często tak się nie dzieje.

Decydując się na hasła jednorazowe, należy zwrócić uwagę na dodatkowy aspekt – finansowy. Urządzenia generujące hasła są drogie, a ich żywotność wynosi kilka lat. Ktoś musi jednak ponieść koszt wysłania SMS-a. Należy podkreślić, że koszty te znikają w przypadku Comarch MobileID, w którym nie ma konieczności wysyłania SMS-ów ani zakupu dodatkowych urządzeń, ponieważ działa on offline na telefonach użytkowników, ale o tym szerzej w kolejnym artykule.

### Podpis elektroniczny

Podpis elektroniczny to kolejna metoda, która może być wykorzystywana do uwierzytelnienia bądź autoryzacji transakcji. Bazuje ona na osiągnięciach kryptografii asymetrycznej. Użytkownik posiada dwa klucze kryptograficzne zależne od siebie – jeden prywatny, drugi publiczny. Klucz prywatny powinien być należycie chroniony przez użytkownika, ponieważ za jego pomocą odszyfrowuje on informacje, które jedynie on powinien przeczytać, oraz może podpisać tekst, dokument, w ogólności jakiś binarny ciąg znaków, potwierdzając jego pochodzenie i swoją wolę. Kryptografia asymetryczna, a w szczególności podpis elektroniczny, zapewnia jednoznaczne potwierdzenie, iż dany podpis został wykonany za pomocą danego klucza, dlatego tak ważna jest jego ochrona przez posiadacza. Za pomocą klucza publicznego można sprawdzić podpis elektroniczny, czyli stwierdzić, iż faktycznie właściciel klucza prywatnego kryptograficznie powiązanego z tym kluczem publicznym złożył dany podpis. Za pomocą klucza publicznego można również zaszyfrować informację, którą po odszyfrowaniu będzie w stanie przeczytać jedynie posiadacz odpowiedniego klucza prywatnego. Algorytmy kryptograficzne asymetryczne, na przykład RSA z kluczem co najmniej 1024-bitowym, są obecnie uważane za bezpieczne. Używanie ich w celach uwierzytelnienia się i autoryzacji jest jak najbardziej polecane. Pamiętaj, że należy jeszcze raz to podkreślić, o odpowiednim zabezpieczeniu samego klucza przed kradzieżą.

### Nowoczesna autoryzacja

Nowoczesna autoryzacja to mechanizmy oparte o pełną infrastrukturę klucza publicznego (PKI), czyli wykorzystujące nie tylko klucze asymetryczne do

podpisu elektronicznego, ale również wprowadzające poświadczenie przynależności klucza publicznego do konkretnej osoby przez zaufaną stronę trzecią, czyli certyfikaty. Mając już certyfikaty, powinno się je wykorzystywać do tworzenia bezpiecznych szyfrowanych połączeń ze stacji użytkownika do docelowej instytucji, obustronnie uwierzytelnionych. Nośnikami kluczy i certyfikatów powinny być dodatkowe fizyczne urządzenia, takie jak karty mikroprocesorowe kryptograficzne czy tokeny USB, będące połączeniem karty mikroprocesorowej kryptograficznej i czytnika w jednym małym urządzeniu. Komponenty służące bezpośrednio do wykonania podpisu powinny być napisane zgodnie z wytycznymi ustawy o podpisie elektronicznym, zgodnie z wytycznymi Komisji Europejskiej, gwarantując najwyższy poziom bezpieczeństwa.

Alternatywą może być stosowanie mechanizmów, które wymuszają na użytkowniku bardziej lub mniej, ale świadome przeniesienie danych transakcji do urządzenia, które wygeneruje na ich podstawie ciąg autoryzacyjny. Czy do końca alternatywą, niektórzy mogą ze mną polemizować. Bezpieczeństwo to zawsze kompromis pomiędzy siłą bezpieczeństwa, kosztami i prostotą użytkownika.

W takim przypadku potwierdzeniu, czyli autoryzacji, podlegają dane podane do urządzenia przez użytkownika, zatem ich podmiana przez złośliwe oprogramowanie na stacji użytkownika nie odniesie pożądanego rezultatu. Haker musiałby wygenerować swój własny kod autoryzacyjny, a to już nie jest takie proste. Atak taki nie powiedzie się.

Już dzisiaj takie urządzenia są dostępne i gotowe do użycia. Wśród nich Comarch MobileID, który pracując w trybie challenge-response, w bezpieczny sposób autoryzuje transakcje, wymuszając na użytkowniku wprowadzenie wybranych cyfr z numeru rachunku i kwoty transakcji. Inne to urządzenia oparte o technologię CAP.

**Chip Authentication Program (CAP)** jest inicjatywą i techniczną specyfikacją firm MasterCard i Visa, mającą na celu wykorzystanie bankowych kart EMV do uwierzytelniania i autoryzacji transakcji on-line. Specyfikacja CAP definiuje urządzenie (tak zwany CAP Reader) posiadające wejście na kartę, klawiaturę składającą się z cyfr oraz wyświetlacz potrafiący wyświetlić co najmniej 12 cyfr. Użytkownik wkłada swoją kartę do czytnika, wpisuje kod PIN do karty, a następnie może wybrać jeden z trzech trybów pracy:

▶ **Identify:** po podaniu kodu PIN czytnik kart na podstawie symetrycznego klucza znajdującego się na karcie generuje jednorazowe hasło, które może zostać użyte do uwierzytelnienia użytkownika.

▶ **Challenge-Response:** użytkownik musi wpisać kod Challenge wyprodukowany przez bank, na podstawie tego kodu oraz klucza symetrycznego czytnik generuje kod response, który może posłużyć do autoryzacji transakcji.

▶ **Sign:** ten tryb jest rozszerzeniem poprzedniego. Oprócz losowego kodu challenge należy wpisać także kluczowe dane transakcji, takie jak: kwota, waluta czy rachunek docelowy. Należy podkreślić, że nazwa sign może być myląca, gdyż w przeciwieństwie do kart kryptograficznych nie jest tutaj tworzony podpis elektroniczny z wykorzystaniem algorytmów asymetrycznych, takich jak RSA lub DSA. Tworzony jest jedynie skrót (najczęściej CBC-MAC/TDES) z podanych danych oraz symetrycznego klucza znajdującego się na chipie. Następnie skrót ten jest transformowany z postaci binarnej do postaci decymalnej, a wybrane cyfry są prezentowane na wyświetlaczu.

Przyszłość to rozwiązania mobilne, również te opisane przeze mnie powyżej. Jednak należy zwrócić uwagę, iż MobileID oraz technologia CAP to nie jest podpis elektroniczny, to nie jest kryptografia asymetryczna. Przyszłość to przeniesienie rozwiązania PKI na urządzenia mobilne, to umożliwienie podpisywania transakcji własnym kluczem prywatnym, w odpowiedni sposób zabezpieczonym przed niepowołanym użyciem. Również w tym zakresie możemy się pochwalić systemem Comarch Mobile PKI, który implementuje podpis elektroniczny i umożliwia jego wykorzystanie na telefonach komórkowych. Karty SIM w polskich telefonach komórkowych nie są jednak jeszcze kartami kryptograficznymi, czyli takimi, które w odpowiedni sposób zabezpieczą klucz prywatny użytkownika, uniemożliwiając wydostanie go na zewnątrz karty. Więcej uwagi tematowi Comarch MobilePKI poświęciliśmy w osobnym artykule tego wydania „Nowych Technologii”.

### Przed czym tak naprawdę musimy się chronić?

Parę informacji, aby nie odbiegać od tematu przewodniego niniejszego artykułu: Jakiego typu ataki są przeprowadzane obecnie na instytucje finansowe i jak należy się przed nimi bronić? Wspomnę te najczęstsze, które bezpośrednio wykorzystują końcowego użytkownika, czyli najsłabsze ogniwo całego systemu teleinformatycznego.

Najprostszym do przeprowadzenia jest atak socjotechniczny, który nie wymaga dodatkowego oprogramowania, ale za to przynajmniej podstawowej wiedzy o atakowanym systemie. Skuteczność takiego ataku jest jeszcze większa, gdy jest on połączony z atakiem „dnia zerowego”, kiedy to

Rysunek 1.

## PRZELEWY

Numer konta docelowego	32 1234 5678 1234 <b>5392</b> 0000 1234
Nazwa właściciela	Jan Kowalski
Adres	Al. Jana Pawła II 39A, Kraków
Kwota	<b>8127,45</b>
Opis	Zasilenie konta

Przepisz podświetlone cyfry do MobileID  
i podaj kod autoryzacyjny

**AUTORYZUJ**



system informatyczny jest uruchamiany i informacje poufne można wyłudzić pod pretekstem testów. Jedyną obroną przed nim są szkolenia wszystkich użytkowników systemu, zarówno tych wewnętrznych, jak i zewnętrznych.

Drugim typem są ataki phishingowe wszelakiego rodzaju. Najczęściej atakujący przygotowuje serwis webowy udający serwisy firm finansowych, na których użytkownicy systemu są proszeni o podanie informacji poufnych. Linki do takich stron są z reguły wysyłane pocztą elektroniczną. Ataki te są powszechne, ponieważ drastycznie rośnie prostota ich wykonywania. Na stronach webowych serwisów rosyjskich można znaleźć gotowe strony, skrypty i komponenty, których można użyć do ataku. Co więcej, strony te zawierają kompletne informacje, mówiące o tym, w jaki sposób można zainstalować takie komponenty na serwerach arabskich bez znajomości alfabetu arabskiego. Filmy instruktażowe poprowadzą domorosłego włamywacza za rączkę, pokazując, co i gdzie należy kliknąć, aby rozpocząć hostowanie serwisu phishingowego. Zainteresowanych zapraszam do bezpośredniego kontaktu. Jak się bronić przed phishingiem? Przede wszystkim szkolić. Istnieją również techniki umożliwiające personalizację stron do logowania. Coraz więcej firm zajmuje się również 24-godzinnym penetrowaniem Internetu w celu wychwytywania stron phishingowych. Potrafią nie tylko odnaleźć takie strony, ale skutecznie je zablokować.

Kolejnym typem są ataki wykorzystujące oprogramowanie zainstalowane na stacji użytkownika końcowego. I jeszcze raz, jedną z podstawowych metod obrony jest podnoszenie wiedzy i świadomości użytkowników, aby mieli zawsze zaktualizowany system operacyjny, zainstalowany program antywirusowy, może nawet firewala, a przede

wszystkim – aby bezzwłocznie nie penetrowali Internetu, pozwalając złośliwemu oprogramowaniu na zainstalowanie się w ich systemie. Ponadto stosowanie nowoczesnych metod autoryzacji i – jeżeli jest to możliwe – stosowanie szyfrowanych połączeń obustronnie uwierzytelnionych pozwoli nam się uchronić przed ewentualnymi problemami.

## Słowo podsumowania

To, jakie metody uwierzytelnienia i autoryzacji powinniśmy zastosować w naszej organizacji, powinno być uzależnione od niebezpieczeństwa na nas czyhającego, z uwzględnieniem ryzyka operacyjnego. Dbanie o odpowiedni poziom bezpieczeństwa powinno być procesem ciągłym, którego zapewnienie winno być monitorowane przez kadrę zarządzającą. Nie należy czekać z założonymi rękami po wprowadzeniu nowoczesnych metod uwierzytelnienia i autoryzacji na sygnał, iż nasze zabezpieczenia po pewnym czasie zostały złamane. Powinniśmy cały czas cyklicznie współdziałać ze specjalistami bezpieczeństwa, którzy będą monitorować stan zabezpieczeń systemów teleinformatycznych i reagować na nowe podatności systemu, na nowinki techniczne, proponując zmiany i udoskonalenia pozwalające spać spokojnie. To, ile powinniśmy zainwestować w bezpieczeństwo, powinno wynikać z analiz:

- ▶ ile możemy stracić, jeżeli nie będziemy posiadać odpowiednich zabezpieczeń,
- ▶ jakie zabezpieczenia, w jakim stopniu niwelują nasze zagrożenia i koszty z nimi związane.

Działy IT są działami kosztowymi – same nie przynoszą zarobku, ale czy na pewno? Nakłady wydane na bezpieczeństwo mogą się okazać kilkakrotnie niższe niż straty, które mogą wynikać z ich braku.

Jedno jest pewne. Inwestycje w bezpieczeństwo powinny być uwzględniane w corocznym budżecie każdej jednostki organizacyjnej. Nowymi technologiami można przyciągnąć nowych klientów, a w oczach obecnych uwiarygodnić się jako strona dokładająca wszelkich starań o ich pieniądze i stosująca zasadę **Prudent Man Rule**.

Wspomniane w niniejszym artykule mechanizmy zabezpieczeń są dostępne w ofercie Comarch.



Tomasz Śnieżyński

Comarch SA

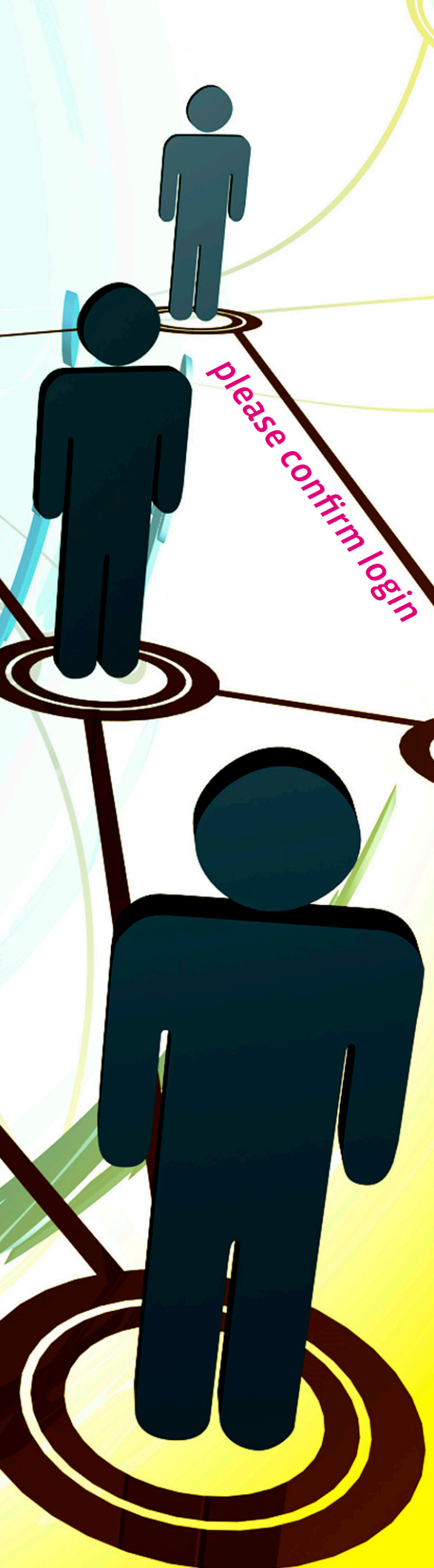
**Stanowisko:** Dyrektor Konsultingu Bezpieczeństwa IT

**Sektor:** Finanse, Bankowość i Ubezpieczenia



# Uwierzytelnienie i autoryzacja transakcji w dobie urządzeń mobilnych

Nie tak dawno możliwości technologiczne, jakie oferowały urządzenia mobilne, sprowadzały się do oglądania prostych stron internetowych z wykorzystaniem przeglądarek WAP. Obecnie rynek zmierza w kierunku wykorzystania przenośnych urządzeń, takich jak Smartphony, urządzenia PDA czy nawet zwykłe telefony komórkowe, w coraz bardziej zaawansowanych biznesowych rozwiązaniach, m.in. bankowości elektronicznej czy systemach maklerskich.



**ANALITYCY** firmy Datamonitor szacują, że w 2012 roku firmy wydadzą na urządzenia mobilne ponad 17 mld USD. To trzykrotnie więcej niż dziś. Jest jednak jedna bardzo poważna bariera hamująca jeszcze większy wzrost tego rynku – bezpieczeństwo. Jest ona szczególnie duża w tak zaawansowanych i wrażliwych systemach jak wspomniane wcześniej rozwiązania bankowe czy maklerskie. Wyniki ostatniego badania firmy McAfee wykazały, że ponad jedna trzecia użytkowników kwestionuje ogólne bezpieczeństwo urządzeń i usług komórkowych. Ponadto 86 proc. użytkowników ma obawy co do potencjalnych zagrożeń, takich jak fałszywe rozliczenia czy kradzież informacji.

– *Przedsiębiorstwa toczą daremną walkę, jeśli chodzi o obecność różnego rodzaju urządzeń mobilnych i nowych technologii w ramach posiadanego środowiska IT* – uważa Daniel Okubo, jeden z autorów raportu. W ramach tego artykułu postaram się skupić na dwóch elementach szeroko rozumianego bezpieczeństwa, mianowicie uwierzytelnieniu osób oraz autoryzacji transakcji, elementach szczególnie istotnych dla rozwiązań, o których już wcześniej wspominałem – bankowości elektronicznej oraz systemów maklerskich. W tym kontekście postaram się pokazać, skąd wynikają obecne ograniczenia i w jaki sposób można spróbować je rozwiązać, aby pokonać tę barierę bezpieczeństwa, stymulując tym samym rozwój technologii mobilnych.

### Metody uwierzytelniania i autoryzacji

Jednym z największych problemów związanych z uwierzytelnieniem i autoryzacją jest brak sprecyzowanych i określonych standardów w kwestii obsługi kodu po stronie klienta (a więc mobilnej przeglądarki internetowej). Tymczasem niemal każda metoda uwierzytelnienia czy autoryzacji takiego kodu potrzebuje. Przedstawię teraz krótko najbardziej popularne metody uwierzytelnienia i autoryzacji oraz ich wymagania co do oprogramowania po stronie klienta. Postaram się też przedstawić inne wady każdej z metod w odniesieniu do urządzeń mobilnych.

**Hasła** – wskazane jest, aby przed przesłaniem hasła siecią wykonać tak zwane skrócenie z wykorzystaniem algorytmów „haszujących”, takich jak SHA1 czy MD5 – a to wymaga kodu JavaScript po stronie klienta.

**Hasła maskowalne** – jeszcze gorzej sprawa wygląda w przypadku haseł maskowanych, bo tutaj oprócz standardowego wysłania hasła potrzebne jest na samym początku wygenerowanie zestawu (zalecane około 200) masek, jest

to algorytmicznie złożona operacja wymagająca sporej mocy obliczeniowej procesora.

**Certyfikaty** – tutaj sprawa się ma najgorzej, gdyż oprócz JavaScript potrzebny jest komponent po stronie klienta w postaci ActiveX lub plugina do innej przeglądarki. Kolejnym problemem jest przechowywanie kluczy prywatnych. Używanie w tym celu dysku uważane jest za niebezpieczne, co zostało potwierdzone wieloma incydentami bezpieczeństwa związanymi z tą metodą. Co prawda główne niebezpieczeństwo wiąże się ze złośliwym oprogramowaniem typu „Koł Trojański”, które jeszcze nie jest tworzone na masową skalę w przypadku urządzeń mobilnych, natomiast z pewnością jest to tylko kwestia czasu i wraz z rozwojem rynku urządzeń mobilnych coraz więcej tego typu oprogramowania będzie powstawać. Jeśli chodzi o urządzenia do bezpiecznego przechowywania kluczy, takie jak tokeny i karty kryptograficzne, zaczynają się pojawiać na rynku w wersji z interfejsem Bluetooth, który umożliwia komunikację z urządzeniami mobilnymi. Niestety jest to na razie raczkujące rozwiązanie i w najbliższym czasie ciężko się spodziewać jego rozpowszechnienia.

**Hasła SMS** – nie wymagają żadnego kodu po stronie klienta i z tego powodu mogą się na początku wydać interesującym rozwiązaniem. Niestety metoda ta posiada dwie bardzo poważne wady. Pierwsza polega na tym, że w przypadku zgubienia lub kradzieży urządzenia osoba, które weszła w posiadanie telefonu, może go bez problemu wykorzystać do przeprowadzenia transakcji, gdyż dostęp do SMS nie jest w żaden sposób zabezpieczony. Drugą wadą jest konieczność przełączania się między aplikacją, w której chcemy dokonać autoryzacji. Część telefonów do tej pory nie ma możliwości wykonania takiej operacji bez zamykania aplikacji, a nawet jeśli mają, to jest to bardzo niewygodne dla użytkownika.

Co prawda JavaScript jest już standardem dla nowych urządzeń mobilnych, ale w przypadku starszych urządzeń dalej pozostaje to problemem. Co więcej, dużą wątpliwość budzi obsługa tego języka skryptowego przez bardzo popularną przeglądarkę Opera Mini. W nowszych wersjach obsługa po stronie klienta jest minimalna, nie ma wsparcia dla skryptów wykonywanych w tle, nie jest obsługiwana większość zdarzeń DOM, wsparcie dla AJAX jest bardzo limitowane. Jeszcze gorzej wygląda sprawa w starszej wersji, gdzie JavaScript po stronie klienta nie jest w ogóle obsługiwany. Całość jest przesyłana do serwera i tam kod jest wykonywany. W przypadku operacji skracania hasła zwy-

Rysunek 1.



klęgo bądź maskowanego musi to budzić poważne zastrzeżenia, gdyż wprowadzamy trzecią stronę transakcji, którą musimy traktować jako zaufaną, co więcej, wysyłamy do tej strony wszystkie hasła nieukrócone, czyli w bardziej wrażliwej formie, niż dostaje docelowy serwis.

Jeszcze gorzej sprawa wygląda z komponentami takimi jak ActiveX. Tutaj o jakimkolwiek wsparciu możemy mówić tylko w przypadku nowych urządzeń. Wymagany jest Internet Explorer Mobile (dostępny od wersji 5.0 Windows Mobile, Pocket Internet Explorer nie ma żadnego wsparcia dla ActiveX). W przypadku przeglądarki Opera w wersji mini nie ma wsparcia dla komponentów po stronie klienta. Wsparcie dla komponentów po stronie klientów pojawiło się w Opera Mobile od wersji 8.65. Należy podkreślić, że wspiera ona ActiveX, a nie Netscape Plugin jak standardowa wersja Opery. Z racji tego Opera zapewnia tylko generyczny interfejs i nie pozwala na tworzenie wielu klas. Jest to tak naprawdę bardzo eksperymentalny projekt, mający na celu zapewnienie wsparcia dla „wtyczek” typu Windows Media Player czy Flash.

### MobilePKI – rozwiązanie na miarę potrzeb

Biorąc pod uwagę te wszystkie zagadnienia, Comarch postarał się wyjść naprzeciw potrze-

bom rynku i proponuje rozwiązania, które w dużej mierze rozwiązują wymienione problemy. Pierwszym produktem jest MobilePKI, które umożliwia korzystanie z infrastruktury klucza publicznego na telefonach komórkowych. Aplikacja oparta jest na aplikacji Java instalowanej na karcie SIM, która zmienia komórkę w przenośną kartę kryptograficzną, zawierającą klucz publiczny i prywatny, niewymagającą czytnika kart do złożenia podpisu. Komunikacja z docelowym systemem (generowanie/aktywacja kluczy/składanie podpisu/uwierzytlenie) odbywa się za pomocą SMS-ów. Należy podkreślić, że rozwiązanie to zapewnia dokładnie taki sam poziom bezpieczeństwa, jeśli chodzi o zabezpieczenie klucza prywatnego, jak normalna karta kryptograficzna. Wykorzystanie tej metody uwierzytelniania oraz autoryzacji nie wymaga korzystania z dodatkowych usług operatora komórkowego, a jedynie wymiany zwykłej karty SIM na kartę z kryptoprocesorem. Generacja kluczy (prywatnego i publicznego) odbywa się na żądanie przychodzące do telefonu z systemu. Po potwierdzeniu przez użytkownika oraz podaniu kodu PIN następuje generacja. Comarch wprowadził dodatkowe zabezpieczenie użycia klucza. Aby system uwierzytelnienia oraz autoryzacji zaczął działać, należy nowo wygenerowany klucz aktywować. Użytkownik końcowy musi na przykład

zadzwoić na infolinię i zgłosić taki fakt operatorowi, który wysyła z systemem transakcyjnego SMS aktywujący. Oczywiście użytkownik może to zrobić osobiście – zależy to już od konkretnego wdrożenia i potrzeby. Podpisanie dokumentu (w szczególności uwierzytlenie i autoryzacja) odbywa się poprzez wysłanie dokumentu na telefon użytkownika z użyciem SMS. Na telefonie wyświetlany jest dokument (mogą to być dane transakcji), który użytkownik może zaakceptować. Po podaniu PIN-u dane są podpisywane i odsyłane do systemu transakcyjnego, który weryfikuje podpis w oparciu o klucz publiczny. Dodatkowo system wspiera tak zwane wsadowe podpisywanie transakcji, czyli podpisywanie zbioru zamiast pojedynczych transakcji. Pozwala to uprościć pracę użytkownika oraz ograniczyć koszty związane z wysyłaniem SMS-ów. Rozwiązanie jest niezwykle obiecujące, gdyż operatorzy komórkowi zapowiadają rychłe wprowadzenie kart z kryptoprocesorem. Ponieważ MobilePKI jest tak zwaną aplikacją SIM Toolkit (jest wgrywana bezpośrednio na kartę SIM), nie wymaga żadnego dodatkowego oprogramowania i może funkcjonować w każdej komórce.

### MobileID, czyli wszechstronność

Drugim rozwiązaniem jest MobileID, czyli token hasel jednorazowych zrealizowany jako aplika-

Rysunek 2.



cja Java na urządzenie mobilne. Co bardzo istotne, urządzenie może pracować zarówno w trybie generacji haseł jednorazowych, jak i w trybie challenge-response. Czyli wiąże konkretną transakcję z wygenerowanym kodem kryptograficznym, zapewniając niezaprzeczalność dokonanej transakcji oraz odporność na ataki typu człowiek w środku, w których intruz wykorzystuje prawdziwe podsłuchane hasło celem autoryzacji fałszywej transakcji. Komponent serwera generuje na podstawie danych z transakcji (numer konta, kwota, bieżący czas lub dowolnych innych) kod autoryzujący, który użytkownik wprowadza do aplikacji na swoim urządzeniu mobilnym. Na jego podstawie generowany jest kod autoryzacyjny response walidowany przez serwer MobileID. Istotną kwestią jest to, że użytkownik, podając PIN do aplikacji, nie wie, czy jest on prawdziwy, gdyż nie jest to sprawdzane po stronie aplikacji klienckiej. Zostaje to zweryfikowane dopiero po stronie serwera, na podstawie wygenerowanego hasła jednorazowego, którego PIN jest składnikiem. Niezwykle ważny jest fakt, iż proces instalacji oprogramowania jest bardzo przyjazny dla użytkownika. Rejestruje się on w systemie, podając swoją nazwę oraz numer telefonu komórkowego, na który zostanie automatycznie wysłana aplikacja w formie WAP-PUSH. Można powiedzieć, że MobileID jest czymś pomiędzy tokenem haseł jednorazo-

wych a SMS-em. Zaletą w stosunku do tych metod uwierzytelnienia jest znacznie niższy koszt takiego rozwiązania, bowiem nie powoduje ono potrzeby wysyłania wiadomości do każdej autoryzacji oraz zakupu dodatkowego urządzenia.

### Nie tylko dla mobilnych

Należy podkreślić, że oba przedstawione mechanizmy uwierzytelniania i autoryzacji transakcji mogą zostać użyte nie tylko w rozwiązaniach mobilnych. Zwłaszcza MobileID nadaje się bardzo dobrze do użycia z rozwiązaniami stacjonarnymi, zastępując sprzętowy token, znacząco redukując koszty, jednocześnie zachowując poziom bezpieczeństwa. Ponieważ MobilePKI zapewnia ten sam poziom bezpieczeństwa co zwykła karta kryptograficzna, może zostać użyty oprócz uwierzytelnienia i autoryzacji transakcji do podpisywania dokumentów (na przykład do ZUS) zgodnie z wymogami rozporządzenia o kwalifikowanym podpisie elektronicznym. Oba rozwiązania spełniają paradygmat uwierzytelnienia wieloczynnikowego przez to, co mam (telefon komórkowy), oraz przez to, co wiem (PIN). Oba rozwiązania radzą sobie z większością problemów omówionych na początku artykułu, takich jak kompatybilność czy skrypty po stronie klienta. Oczywiście nie rozwiązują wszystkich bolączek uwierzytelnienia i autoryzacji dla urządzeń

mobilnych, a tym bardziej wszystkich bolączek bezpieczeństwa w szerszym kontekście, ale są krokiem w dobrą stronę i mogą stać się przyczynkiem do jeszcze szybszego rozwoju rynku urządzeń mobilnych oraz usług biznesowych oferowanych za ich pośrednictwem.



**Maciej Wolański**

Comarch SA

**Stanowisko:** Konsultant ds. Bezpieczeństwa

**Sektor:** Finanse, Bankowość i Ubezpieczenia

# Zarządzanie dostępem i tożsamością

**KORZYŚCI DLA UŻYTKOWNIKÓW I ADMINISTRATORÓW**

Odkąd powstała pierwsza aplikacja, z której mógł korzystać nie tylko jeden użytkownik, powstał problem w ich rozróżnianiu. Zadawano pytania, po co należałoby różnicować użytkowników, w jakich przypadkach, według jakich kryteriów, jak zarządzać uprawnieniami użytkowników? Wszystkie te pytania sprowadzały się tak naprawdę do jednego – w jaki sposób kontrolować dostęp do systemów teleinformatycznych i zarządzać nim.



START

**PIERWSZE** aplikacje były dostarczane z wbudowanymi kontami dla użytkowników, którzy w zależności od podanej nazwy mieli dostęp do konkretnych, zdefiniowanych funkcjonalności. Było to bardzo uciążliwe, ponieważ każda zmiana w aplikacji niosła za sobą konieczność zmian w module odpowiedzialnym za dostęp do aplikacji. Z biegiem czasu i postępu informatyzacji, kiedy to komputery wyszły z pojedynczych pomieszczeń, najczęściej uniwersyteckich, i zaczęły wchodzić do coraz nowszych gałęzi gospodarki, aplikacje stawały się wciąż potężniejsze, wymagające obsługi dużej liczby użytkowników. Wymuszało to na projektantach tworzenie architektur pozwalających na łatwy przyrost liczby użytkowników. Szybko zaczęto wykorzystywać zewnętrzne bazy danych, drzewa katalogowe, które przechowywały informacje o użytkownikach. Powstawały również standardy przechowywania uprawnień użytkowników oraz modele zarządzania dostępem. W niniejszym artykule przedstawię podstawowe modele z perspektywy użytkownika i administratora oraz pokażę przyczyny konieczności stosowania mechanizmów zarządzania tożsamością w dużych systemach IT.

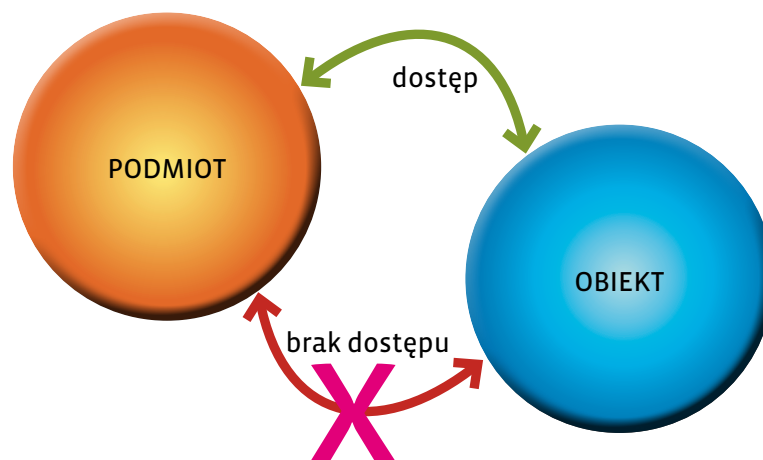
### Zarządzanie dostępem – autoryzacja

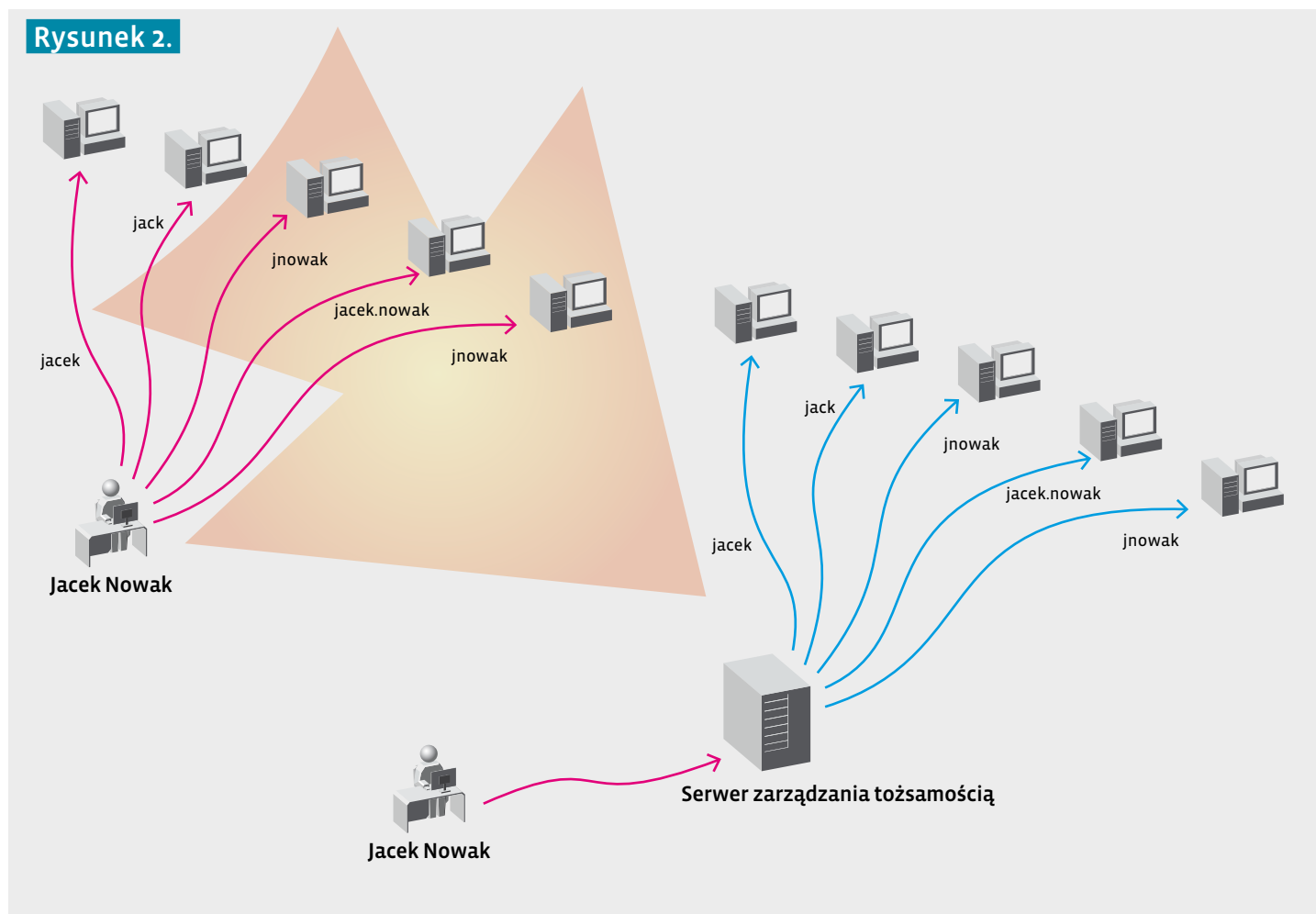
W zarządzaniu dostępem mówimy zawsze o dostępie czegoś do czegoś. Coś, co żąda dostępu, nazywamy podmiotem, zaś coś, do czego dostęp jest żądany, **obiektem**. Między podmiotem a obiektem musi istnieć mechanizm, który na podstawie pewnych zapisów – reguł określi, czy dany podmiot może uzyskać dostęp do obiektu, czy też nie. Z punktu widzenia tychże reguł w zarządzaniu dostępem można wyróżnić trzy modele.

**Pierwszym modelem**, o jakim powiem, jest **mandatory access control (mac)**, co w wolnym tłumaczeniu brzmi: obligatoryjna bądź narzucona kontrola

dostępu. Każdy obiekt posiada etykietkę związaną z jego klasyfikacją na poziom bezpieczeństwa lub oznaczeniem wrażliwości danych, które dany obiekt przechowuje. Każdy podmiot, który chce uzyskać dostęp do takiego obiektu, musi posiadać również odpowiednią etykietkę, tak zwane poświadczenie bezpieczeństwa dla danego poziomu. Klasyfikacje mogą być różne. Instytucje rządowe są na przykład zobligowane ustawą o informacjach niejawnych do stosowania następującej nomenklatury: informacje jawne, zastrzeżone, tajne i ściśle tajne. Podmiot mający poświadczenie bezpieczeństwa na poziomie tajne może uzyskać dostęp do poziomu o tej samej kwalifikacji lub niższych. Dostęp w tym modelu jest często związany z dodatkowymi restrykcjami. Z reguły restrykcją jest paradygmat bezpieczeństwa **need-to-know**. Polega on na tym, iż podmiot niezależnie od posiadanego poświadczenia bezpieczeństwa musi mieć uzasadnioną potrzebę do korzystania z zasobów danego obiektu, wynikającą na przykład z jego obowiązków służbowych. Przykładem modelu mac jest mechanizm **rule-based access control**, czyli zarządzanie dostępem poprzez reguły, ponieważ to reguły determinują dostęp podmiotu do obiektu. Podsumowując, jak działa ten model z punktu widzenia użytkownika i administratora? Administratorem w tym przypadku jest właściciel obiektu, czyli właściciel informacji, ponieważ to on klasyfikuje swoje obiekty, nadając im odpowiedni poziom bezpieczeństwa. Może być pewny, że nikt o niższym poświadczeniu bezpieczeństwa nie będzie miał dostępu do jego danych. Należy wprost podkreślić, iż nie steruje on bezpośrednio dostępem do obiektów, jedynie je klasyfikuje. A użytkownik musi zdobyć odpowiednie poświadczenie i dodatkowo posiadać potrzebę dostępu do danego obiektu. W przeciwnym razie dostęp zostanie mu odmówiony.

**Drugim modelem** jest **discretionary access control (dac)**, co tłumaczymy jako swobodną kontrolę dostępu. W tym przypadku właściciel informacji





ma możliwość swobodnego zarządzania dostępem do swoich obiektów, dla konkretnych użytkowników. Przykładem implementacji tego modelu jest tworzenie list kontroli dostępu (ang. acl), które zawierają powiązanie uprawnionego użytkownika z obiektem, często konkretnym plikiem. Model ten z jednej strony daje dużą swobodę i precyzję nadawania uprawnień do plików, ale z drugiej wymaga starannego zarządzania. Najczęściej o dostępie decyduje jedynie sama tożsamość danego podmiotu, mówimy wtedy o **identity-based discretionary access control**. Niekiedy kontrola nad dostępem do obiektów może zostać udostępniona użytkownikom bezpośrednio. Mamy wtedy do czynienia z user-direct discretionary access control.

**Kolejny model to non-discretionary access control (n-dac)**, czyli kontrola dostępu narzucona. W tym przypadku decyzja o dostępie jest podejmowana centralnie, autorytatywnie, często w nawiązaniu do polityki bezpieczeństwa danej organizacji. Zarządzanie dostępem może bazować na przynależności użytkownika do tak zwanej roli. Role mogą być tworzone w oparciu o funkcje, z którymi związane są określone akcje użytkowników, czyli ich zakres

obowiązków w organizacji. Przynależność użytkownika do roli determinuje jego zestaw uprawnień do obiektów. Taki model nazywamy **role-based access control**. Nazwa ta stosowana jest często wymienne z nazwą samego modelu (n-dac). Można również wyróżnić w tym modelu szeregowanie użytkowników względem powierzonych im obowiązków. Mówimy wtedy o modelu **task-based access control**. Model n-dac jest bardzo wygodny w użyciu dla dużych systemów, w którym mamy do czynienia z dużą rotacją użytkowników. Poprzez szybkie dodanie użytkownika do odpowiedniej roli, wynikającej z jego służbowych obowiązków, można mu nadać wszelkie niezbędne w jego pracy uprawnienia. Codzienna administracja takiego systemu jest więc bardzo prosta. Skupienia i uwagi wymaga jedynie okres tworzenia takiego systemu, kiedy to projektant aplikacji musi odpowiednio skonstruować system ról powiązany z określonymi funkcjonalnościami.

### Zarządzanie tożsamością

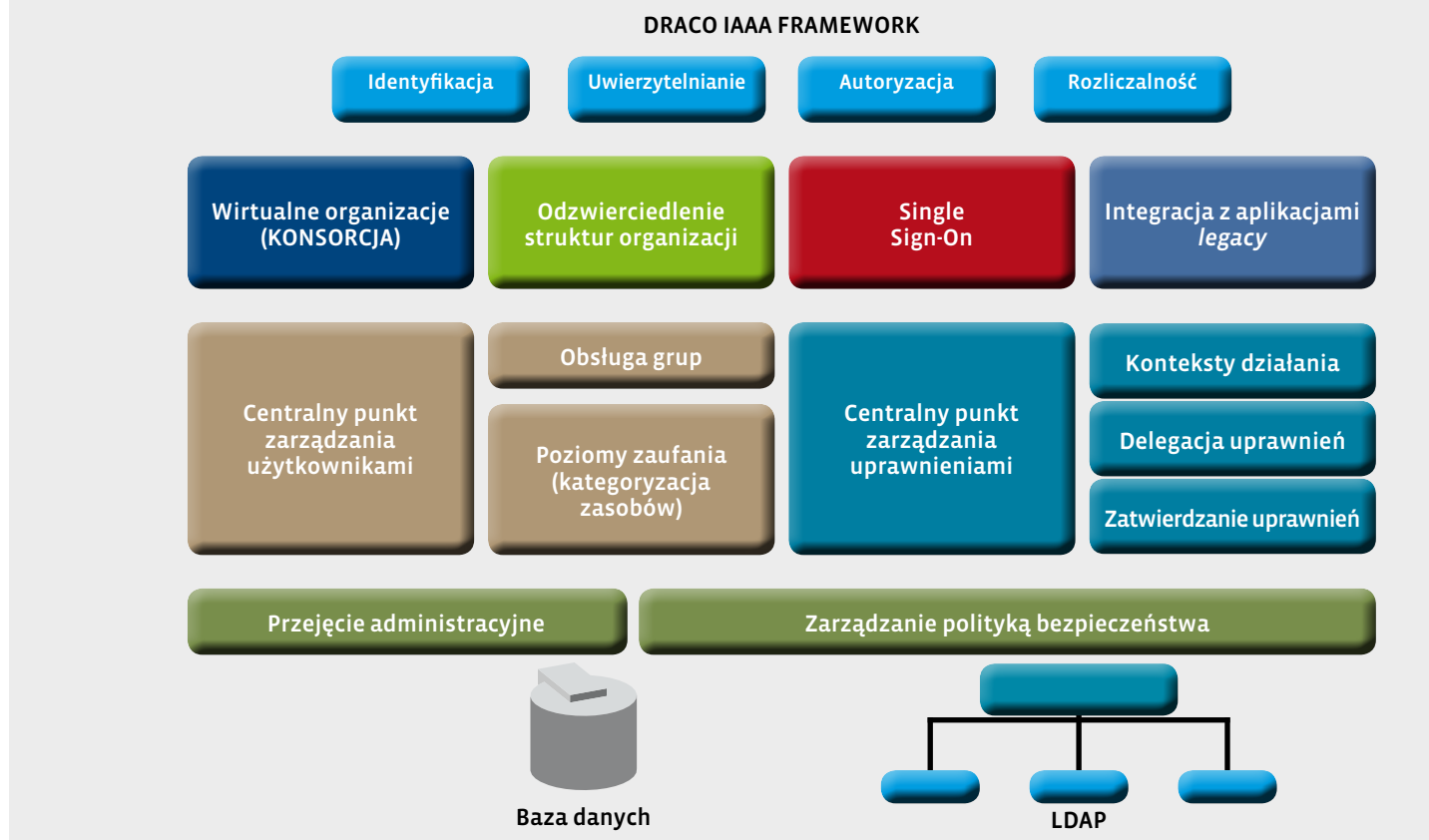
Powyżej przedstawiłem modele zarządzania dostępem podmiotów do obiektów, czyli tak naprawdę

modele autoryzacji. W pojęciu zarządzania dostępem kryje się jeszcze jeden element – uwierzytelnienie. Każdy podmiot przed przystąpieniem do fazy autoryzacyjnej musi zostać zidentyfikowany, a jego tożsamość potwierdzona. Istnieje wiele metod uwierzytelnienia, jednak w tym artykule nie będziemy o nich wspominać. Najważniejsze jest, iż każdy system powinien wymagać uwierzytelnienia. Problem zaczyna się pojawiać w chwili, gdy w środowisku IT pracuje wiele systemów, zależnych lub niezależnych od siebie. Pojedynczy użytkownik w danej organizacji może mieć nawet do kilku kont, czyli w najgorszym przypadku kilka różnych nazw użytkownika i kilka różnych metod uwierzytelnienia. Do takich środowisk niezbędne jest wprowadzenie systemu zarządzania tożsamością użytkownika, który najczęściej powiązany jest z funkcjonalnością jednokrotnego logowania się (ang. single sign-on). Co nam to daje? Poniżej wymienione są najważniejsze korzyści z wdrożenia takiego systemu.

Z punktu widzenia użytkownika:

- ▶ Użytkownik posiada dostęp do różnych systemów, jednak identyfikuje się tym samym user-name'em.

**Rysunek 3. Comarch Security Access Manager – DRACO to system klasy Access Management i Identity Management. Schemat ukazuje jego najważniejsze bloki funkcjonalne.**



- ▶ Użytkownik, uwierzytelniając się raz, uzyskuje dostęp do wszystkich systemów wewnątrz środowiska IT.
- ▶ Użytkownik nabiera przekonania o wysokim poziomie IT governance, co może być również ważnym argumentem podczas podejmowania decyzji o zakupie takiego systemu.

Z punktu widzenia administratora:

- ▶ W końcu administrator ma całościową informację, ile kont posiada dana fizyczna osoba w całym środowisku IT.
- ▶ Zarządzanie wszystkimi kontami w różnych systemach odbywa się z jednego, centralnego miejsca.
- ▶ Zarządzanie dostępem użytkowników do obiektów, w zależności od wybranego modelu, odbywa się z jednego, centralnego miejsca.
- ▶ Administrator ma możliwość wygenerowania zbiorczego raportu o działalności użytkownika w całym środowisku IT.
- ▶ Administrator ma możliwość zablokowania/usunięcia wszystkich kont użytkownika z jednego,

centralnego miejsca, za pomocą jednego przycisku, w całym środowisku IT.

- ▶ Wprowadzenie systemu zarządzania tożsamością niesie przede wszystkim zmniejszenie kosztów utrzymania systemów, co związane jest z uproszczoną administracją.

### Podsumowanie

Nowoczesny system zarządzania dostępem powinien umożliwiać zarówno zarządzanie uwierzytelnieniem, autoryzacją poprzez możliwość obsługi różnych modeli dostępu, jak i tożsamością. Comarch Security Access Manager (DRACO) jest właśnie takim systemem. Niesie ze sobą nowoczesną technikę oraz nowoczesne mechanizmy zarządzania. Wszystkie wspomniane w niniejszym artykule mechanizmy są zaimplementowane w tym systemie. Poprzez obsługę różnych modeli kontroli dostępu DRACO znajduje swoje zastosowanie zarówno w jednostkach organizacji rządowych, jak i w firmach komercyjnych. Serdecznie zapraszam do lektury kolejnego wydania *Nowych Technologii*, w którym tematyce zarządzania tożsamością poświęcimy więcej uwagi.



**Tomasz Śnieżyński**

Comarch SA

**Stanowisko:** Dyrektor Konsultingu Bezpieczeństwa IT

**Sektor:** Finanse, Bankowość i Ubezpieczenia

# Niebezpieczeństwa płynące z sieci wewnętrznej korporacji

Na dzisiejszym rynku, a zwłaszcza na rynku związanym z nowoczesnymi technologiami, wartość informacji jest coraz większa w stosunku do zasobów materialnych posiadanych przez firmę i trend ten stale rośnie.

**SZACUJE** się, że w roku 2007 na świecie znajdowało się około 281EB informacji (1 Eksabajt to 1024\*1024\*1024 GB), co daje 45GB informacji na każdego człowieka na Ziemi. Co więcej, według raportu IDC „The Diverse and Exploding Digital Universe: An Updated Forecast of Worldwide Information Growth Through 2011” (Zróżnicowany i eksplodujący wszechświat cyfrowy: zaktualizowana prognoza wzrostu ilości informacji na świecie do roku 2011) w 2011 ilość ta wzrosła do 1,8ZB (1 Zettabajt to 1024 Eksabajtów). Pomimo że połowa tych informacji jest wynikiem działań indywidualnych ludzi (takich jak zdjęcia cyfrowe itd.), to przedsiębiorstwa są odpowiedzialne za bezpieczeństwo ponad 85 proc. tych informacji. *W miarę jak rośnie ilość śladów cyfrowych pozostawianych przez ludzi, rosnąć też będzie odpowiedzialność przedsiębiorstw i instytucji za prywatność, ochronę, dostępność oraz rzetelność tej informacji. Działania informatyczne przedsiębiorstw będą musiały stawić czoła problemom związanym z ryzykiem, zgodnością z przepisami, niewłaściwym użyciem informacji, wyciekami danych oraz ochroną przed naruszeniami bezpieczeństwa* – powiedział Joe Tucci, przewodniczący rady nadzorczej, prezes zarządu i dyrektor generalny EMC.

### Wartość informacji

Skoro znamy już szacunki co do ilości informacji na świecie, spróbujmy zdefiniować jeszcze pojęcie wartości informacji. Istnieje wiele formalnych, jak i nieformalnych definicji, jedną z najpopularniejszych jest „wartość informacji jest równa cenie, jaką osoba potrzebująca takiej informacji jest skłonna zapłacić”. Ja osobiście nie lubię tej definicji, ponieważ dla każdego dana informacja może mieć zupełnie inną wartość. Znacznie bardziej trafiona wydaje mi się definicja, która mówi, że „wartość informacji jest równa sumie strat, jaką może spowodować niedostępność, utrata, kradzież lub zafałszowanie tej informacji”. Straty takie można podzielić na bezpośrednie, wynikające na przykład z defraudacji lub z działalności konkurencji wykorzystującej ukradzione informacje. Drugą kategorią są straty pośrednie, takie jak na przykład utrata reputacji w wyniku przeprowadzonego ataku. Należy podkreślić, że według badań statystycznych większość zagrożeń dla informacji pochodzi z sieci wewnętrznej, co więcej nie muszą to być celowe działania. Wiele takich zagrożeń wynika z niedbałości lub niewiedzy użytkowników sieci wewnętrznej. Dlatego jednym z podstawowych celów każdej z korporacji powinno być zabezpieczenie danych przed utratą, kradzieżą oraz zafałszowaniem, jak mówi Mark Lewis, wiceprezes wykonawczy i dyrektor ds.

rozwoju firmy EMC Corporation w wyżej już wspomnianym raporcie: *Biorąc pod uwagę, że odpowiedzialność za 85 proc. tworzonych i kopiowanych informacji będą ponosić organizacje i przedsiębiorstwa, musimy jako branża podejmować kroki, które zapewnią nam opracowanie elastycznych, godnych zaufania i bezpiecznych infrastruktur informatycznych, które będą w stanie przetworzyć rosnącą ilość przepływających informacji. Potrzebna nam będzie jeszcze jedna definicja, bo co to właściwie znaczy, że informacja jest bezpieczna? Jak powszechnie wiadomo, żaden system nie może być w pełni bezpieczny, zawsze istnieją jakieś luki, bądź to w oprogramowaniu, bądź w procedurach, czy wreszcie po prostu błędy lub celowe działania ludzi, którzy system obsługują. Idealną definicją na potrzeby tego artykułu będzie: „informację uważamy za bezpieczną, jeśli koszty poniesione na kradzież, zafałszowanie lub spowodowanie utraty są wyższe niż potencjalne zyski dla osoby próbującej taką operację przeprowadzić”.*

### Bezpieczna korporacja

Jak ten cel zrealizować? Podstawą bezpieczeństwa w każdej korporacji jest dobrze zdefiniowana polityka bezpieczeństwa, niestety w większości przypadków jest to martwy dokument. Istnieje wiele sposobów wspomaganie realizacji polityki bezpieczeństwa, takich jak szkolenia, audyty, kontrola wewnętrzna i najważniejsze ze wszystkich – narzędzia. Sama polityka bezpieczeństwa oraz metody jej wymuszania są tematem na osobny artykuł, w tym spróbuję przedstawić jedno z narzędzi autorstwa firmy Comarch, którego celem jest zabezpieczenie informacji zgromadzonych w wewnętrznej infrastrukturze korporacji.

*SecureAdmin to system monitorowania aktywności użytkowników działający w sposób przezroczysty na poziomie warstwy sieciowej. Cechy te oznaczają, że wdrożenie systemu SecureAdmin nie wymaga modyfikowania ani rekonfigurowania istniejących aplikacji lub systemów, a jego obecność nie jest widoczna dla użytkowników. Dzięki temu jest to doskonały system uzupełniający monitorowanie aktywności użytkowników wykonywane w oparciu o logi aplikacyjne i systemowe lub też do monitorowania aktywności administratorów* – mówi Roman Lewandowski odpowiedzialny za stworzenie pierwszej wersji systemu, który wraz z Michałem Zalewskim, autorem książki „Cisza w Sieci”, był pomysłodawcą systemu.

### Życie z SecureAdmin

System ma dwie unikalne cechy. Pierwsza to jego przezroczystość – jest to urządzenie drugiej warstwy sieciowej (działa jak bridge lub switch), a więc

Tabela 1.

Protokół	Zapisywane informacje
HTTP	Nagłówki żądań i odpowiedzi HTTP
FTP	Polecenia i odpowiedzi przesyłane w połączeniu kontrolnym FTP
telnet	Polecenia wykonywane przez użytkownika i odpowiedzi serwera
SSH (szyfrowany)	
POP3	Wykonane polecenia i status ich wykonania, bez zawartości odbieranej poczty. Z technologicznego punktu widzenia jest to możliwe, natomiast z przyczyn etycznych z reguły ta możliwość jest wyłączana
IMAP	
SMTP	Z technologicznego punktu widzenia jest to możliwe, natomiast z przyczyn etycznych z reguły ta możliwość jest wyłączana
SMB	Operacje wykonane na plikach lub katalogach i status ich wykonania, bez zawartości plików. Podobnie jak w przypadku protokołów pocztowych istnieje możliwość zapisywania plików, natomiast z reguły jest to wyłączone z powodu dużej ilości miejsca, jakie te pliki by zajmowały
NFS	
Oracle	Wykonane zapytania SQL i status ich wykonania (pomyślny lub błąd) – bez danych. Podobnie jak w przypadku protokołów pocztowych istnieje możliwość zapisywania danych, natomiast z reguły jest to wyłączone z powodu dużej ilości miejsca, jakie te pliki by zajmowały
MySQL	
PostgreSQL	
MsSQL	
X11 (szyfrowany)	Zrzuty ekranu wykonywane w konfigurowalnych odstępach czasu. Zapis klawiszy naciskanych przez użytkownika
SSL	Daje możliwość analizowania wszystkich protokołów nieszyfrowanych, tunelowanych z wykorzystaniem SSL
Dowolny protokół	System SecureAdmin posiada API, za pomocą którego można stworzyć analizator dowolnego protokołu. Dzięki temu korporacje dostają możliwość monitorowania własnych zamkniętych protokołów

jego wdrożenie jest zupełnie przezroczyste dla istniejących w korporacji systemów. Cecha ta jest łatwa do osiągnięcia dla podsłuchiwanie pakietów nieszyfrowanych, gdyż wówczas pakiety przesyłane w połączeniach nie są w żaden sposób modyfikowane. Wyjątkowość systemu SecureAdmin polega na zapewnieniu przezroczystości również w trybie analizowania połączeń przy wykorzystaniu metody Man In The Middle (MITM). W tym trybie system z wykorzystaniem mechanizmów IPTables przekazuje połączenie na lokalny port i symuluje nawiązanie połączenia klienta, natomiast sam nawiązuje połączenie z serwerem w imieniu klienta. Sensor podszywa się pod adresy IP prawdziwego serwera

i klienta, tak że jego obecność jest niewidoczna zarówno dla klienta, jak i serwera.

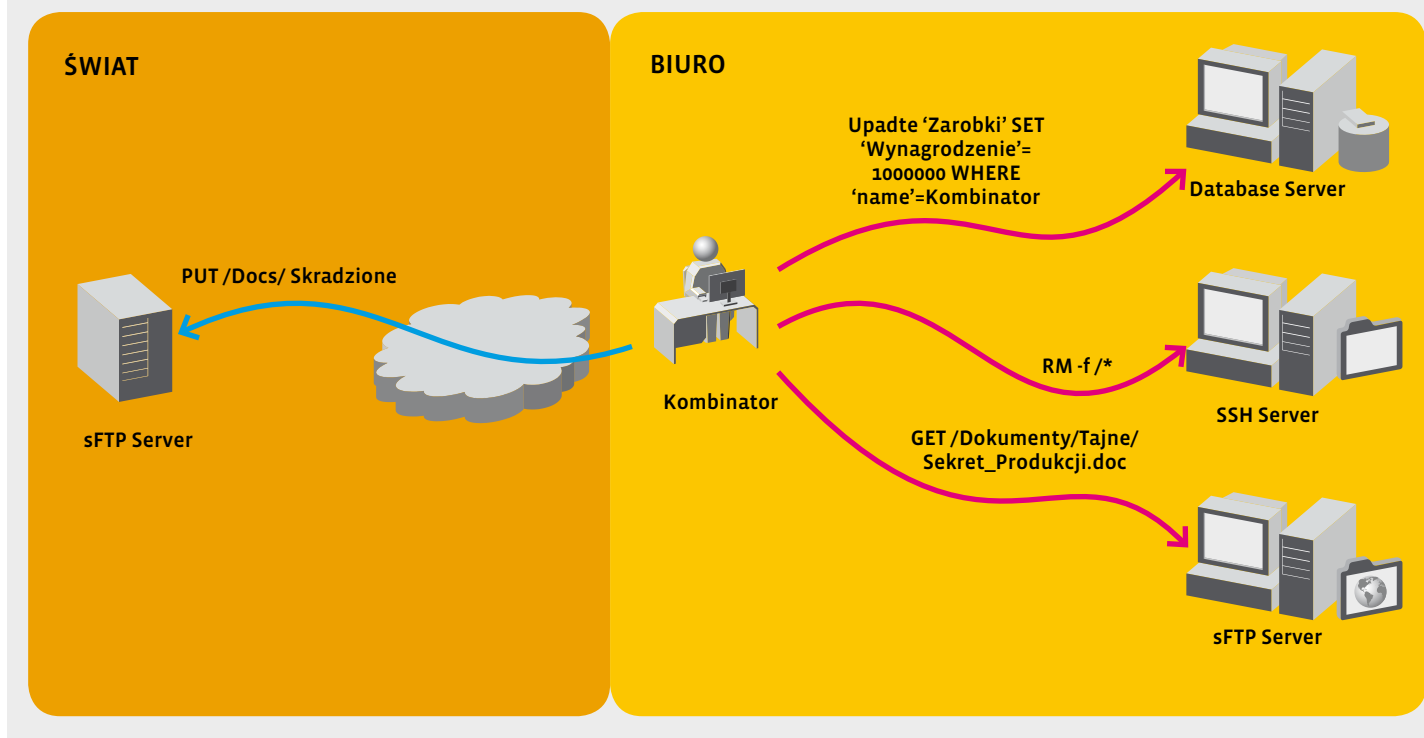
Możliwość analizowania ruchu szyfrowanego jest kluczowa z punktu widzenia bezpieczeństwa wewnętrznego, gdyż pracownicy coraz częściej wykorzystują możliwość tunelowania protokołów nieszyfrowanych z wykorzystaniem szyfrowanych, celem oszukania istniejących w sieci mechanizmów zabezpieczających i monitorujących. Obecnie SecureAdmin obsługuje protokoły sieciowe przedstawione w tabeli.

Analizatory poszczególnych protokołów są łądowane jako osobne, niezależne od siebie moduły. Dzięki temu możliwe jest dodawanie nowych ana-

lizatorów bez przerywania pracy pozostałych oraz, w razie potrzeby, stworzenie modułów dla nowych protokołów bez ingerowania w system. Dodatkowo SecureAdmin udostępnia API, dzięki któremu każdy może stworzyć analizator nowego protokołu. Jest to szczególnie istotne w przypadku korporacji, które wykorzystują własne zamknięte protokoły; dzięki zastosowanemu mechanizmowi mogą same stworzyć wymagane analizatory.

Celem monitorowania ruchu sieciowego i analizowania protokołów w systemie SecureAdmin jest rejestrowanie aktywności użytkowników. Oznacza to, iż dla większości protokołów nie są rejestrowane wszystkie bajty przesłane w monitorowa-

Rysunek 1.



nym połączeniu (choć jest to możliwe, jeśli zostanie zapewniona odpowiednia infrastruktura informatyczna umożliwiająca przechowywanie i przetwarzanie takiej ilości informacji), a jedynie informacje o aktywności użytkowników, czyli o wykonanych przez nich czynnościach oraz ich rezultatach. Oprócz informacji szczególnych dla każdego analizowanego połączenia przedstawionych w tabelce rejestrowane są następujące informacje:

- ▶ czas rozpoczęcia połączenia,
- ▶ czas trwania połączenia,
- ▶ źródłowy i docelowy adres MAC,
- ▶ źródłowy i docelowy adres IP wraz z portem,
- ▶ źródłowy i docelowy adres,
- ▶ typ protokołu,
- ▶ nazwa użytkownika i hasło (o ile są dostępne).

System SecureAdmin posiada moduł wysokiej dostępności (HA), który poprzez zastosowanie redundantnej architektury składającej się z dwóch serwerów działających w trybie fail-over zapewnia ciągłość pracy w przypadku awarii jednego z serwerów. Dzięki tej funkcjonalności w momencie wykrycia awarii jednego z serwerów możliwe będzie automatyczne przełączenie komunikacji na drugi serwer, należy podkreślić, że wszystkie aktywne sesje użytkownika zostaną przeniesione na drugi serwer, umożliwiając kontynuowanie pracy bez

konieczności nawiązywania nowej sesji. Opisaną dodatkową funkcjonalnością niezbędną przy tego typu systemie jest wbudowany elastycznie konfigurowalny system powiadomień, pozwalający na szybką reakcję na incydenty bezpieczeństwa. SecureAdmin jest w stanie reagować na zdarzenia, wysyłając SMS-y, e-maile, powiadomienia WWW lub tak zwane trapy Simple Network Management Protocol (SNMP), które pozwalają na poinformowanie o zaistniałej sytuacji innych urządzeń sieciowych.

## Podsumowanie

Podsumowując, system SecureAdmin nie jest remedium na wszelkie problemy z bezpieczeństwem w sieci korporacyjnej. Jest natomiast znakomitym narzędziem wspomagającym egzekwowanie polityki bezpieczeństwa i wykrywanie jej naruszeń, zarówno przypadkowych, jak i umyślnych. Produkt ten pozwala także uniknąć bardzo niebezpiecznej sytuacji, w której administrator może zrobić wszystko wewnątrz sieci, a oprócz tego zamazać swoją działalność. SecureAdmin znacząco ogranicza możliwość wykonania anonimowo szkodliwego działania, co jest doskonałym środkiem prewencyjnym, który znacząco podnosi poziom bezpieczeństwa składanych informacji. Przyczynia się to do możliwości opracowania elastycznych, godnych

zaufania i bezpiecznych infrastruktur informatycznych, które będą w stanie przetworzyć rosnącą ilość przepływających informacji.



### Maciej Wolański

Comarch SA

**Stanowisko:** Konsultant ds. Bezpieczeństwa

**Sektor:** Finanse, Bankowość i Ubezpieczenia

# Ubezpieczenia zdrowotne – nowe rozwiązania systemowe

COMARCH HEALTH INSURANCE JAKO ODPOWIEDŹ NA POTRZEBY RYNKU

## Publiczna opieka zdrowotna a ubezpieczenia prywatne w Europie

Mimo zapewnionej publicznej służby zdrowia w każdym z krajów europejskich zainteresowanie prywatną opieką medyczną jest duże. Nie jest to tylko związane ze słabym systemem publicznym w niektórych krajach, który nie pokrywa 100 proc. zapotrzebowania obywateli na usługi medyczne i operacje, ale przede wszystkim wynika ze wrażliwej świadomości co do potrzeb ochrony własnego zdrowia i zdrowia bliskich. W hierarchii wartości zdrowie niejednokrotnie jest wymieniane na pierwszym miejscu, często przed miłością i przed pieniędzmi.

W całej Europie zauważalny jest problem starzejącego się społeczeństwa. Średnia długość życia wydłuża się, a wskaźnik urodzeń maleje. Powoduje to, że finansowanie publicznej służby zdrowia jest coraz trudniejsze. Z danych OECD wynika, że za dwa lata jedna czwarta Europejczyków będzie po sześćdziesiątce. Już dziś w Europie Zachodniej wydatki na służbę zdrowia wynoszą 10-15 proc. GDP i rosną w tempie 7 proc. rocznie. W Europie Centralnej i Wschodniej finansowanie publicznej służby zdrowia jest na wiele niższym poziomie – w Polsce w 2007 roku udział wydatków na opiekę medyczną wyniósł 6,5 proc. GDP. Natomiast wg danych WHO (*World Health Organization*) wydatki na opiekę zdrowotną na Ukrainie w 2001 i 2002 roku stanowiły zaledwie 3,4 proc. GDP. W tym czasie średnia europejska zbliżała się do 9 proc. GDP.

W 2007 roku Polacy na prywatne usługi i produkty medyczne wydali około 20 mld PLN, co stanowi aż około 30 proc. szacowanego na ponad 61 mld PLN rynku świadczeń medycznych w Polsce. W ciągu ostatnich dziesięciu lat prywatne wydatki Polaków na ochronę zdrowia wzrosły o ponad 70 proc., zaś w roku 2007 wydatki te wzrosły o około 13 proc. w porównaniu do poprzedniego roku, co znacznie przewyższa wskaźnik GDP. Ponad połowa tych wydatków przeznaczana była na sprzęt medyczny i leki. Jednak to wydatki na ubezpieczenia zdrowotne i abonamenty medyczne charakteryzują się obecnie najwyższą dynamiką. Na upowszechnianiu prywatnego leczenia w Polsce korzystają nie tylko firmy ubezpieczeniowe, ale i same placówki medyczne. Obroty prywatnych firm oferujących usługi medyczne rosną obecnie bardzo szybko. Największe z nich odnotowały w ubiegłym roku rekordowe 30-40-proc. wzrosty przychodów.

Zainteresowanie Polaków ubezpieczeniami zdrowotnymi jest duże, a przewiduje się, że w najbliższych latach oprócz podstawowych usług medycznych, tj. wizyt lekarskich i usług diagno-

### Prognozy dotyczące polskiego rynku ubezpieczeń zdrowotnych

Polska Izba Ubezpieczeń szacuje, że w ciągu najbliższych 5 lat 15 proc. społeczeństwa polskiego będzie posiadało prywatne ubezpieczenia zdrowotne (to jest ok. 5,8 mln pacjentów). Przy założeniu, że składka dodatkowa (opłacana z własnej kieszeni przez pacjentów) dla każdej grupy wiekowej średnio wyniesie 600 zł rocznie (50 zł miesięcznie), szacuje się, że wielkość rynku prywatnych ubezpieczeń zdrowotnych wyniesie 8,4 mld zł rocznie.

stycznych, będzie wzrastało zapotrzebowanie na pakiety szpitalne.

Na Ukrainie także odnotowuje się wzrost zainteresowania prywatnymi ubezpieczeniami zdrowotnymi. Przypis składki z ubezpieczeń wypadkowych i zdrowotnych łącznie (A&H – accident and health) wzrósł z 520,08 mln UAH do 723,38 mln UAH w 2006 roku (wzrost o 39 proc.). Wzrósł także udział tych ubezpieczeń w całym portfelu ubezpieczeń majątkowych z 4,2 proc. w 2005 roku do 5,4 proc. w 2006 roku. W ubezpieczeniach A&H (do których zalicza się wypadkowe, zdrowotne, chorobowe i wydatki medyczne) – największy udział mają właśnie ubezpieczenia zdrowotne – wyniosły one w 2006 roku 362,328 mln UAH, co daje wzrost aż o 42 proc. w porównaniu do roku 2005 (254,935 mln UAH). Spośród innych ubezpieczeń majątkowych na Ukrainie – ubezpieczenia zdrowotne charakteryzują się jednym z wyższych wskaźników dynamiki.

### Przesłanki do rozwoju ubezpieczeń zdrowotnych

W obliczu niezadowalającej sytuacji publicznej służby zdrowia w Polsce i innych krajach europejskich rynek ubezpieczeń zdrowotnych będzie się nadal rozwijał. Jest na to przyzwolenie społeczne i rządowe. Pacjenci nie chcą, a często nie mogą pozwolić sobie na czekanie w długich kolejkach do lekarzy specjalistów czy na operacje. Wielu jest gotowych płacić więcej za wyższy standard opieki. Państwo natomiast zmuszone jest szukać dodatkowych źródeł finansowania opieki medycznej i w dobrowolnych dodatkowych ubezpieczeniach zdrowotnych upatruje szansy na poprawę sytuacji finansowej publicznej służby zdrowia. Dodatkowym czynnikiem sprzyjającym rozwo-

jowi ubezpieczeń prywatnych jest stworzona już sieć prywatnych placówek medycznych, które świadczą zarówno usługi medyczne prywatnie, jak i w ramach społecznych ubezpieczeń zdrowotnych. Firmy ubezpieczeniowe współpracujące z placówkami medycznymi od dawna już oferują różne warianty ubezpieczeń zdrowotnych ze względu na kieszeń i potrzeby klientów. Różnorodność wariantów i ilość ofert na rynku ubezpieczeniowym będzie rosła, w miarę jak nowe usługi medyczne będą rozpowszechniane. Medycyna należy do jednej z szybciej zmieniających się dziedzin – w leczeniu chorób pojawiają się nowe podejścia, opracowywane są nowe szczepionki, zaleca się coraz więcej form rehabilitacji i poprawy stanu zdrowia. Przy tym wszystkim zagrożenie chorobami w obecnym wieku wcale nie maleje, wprost przeciwnie – „nowoczesny styl życia” sprzyja tworzeniu się nowych dolegliwości. Świadomość społeczeństwa dotycząca zagrożeń jest duża, a dbałość o stan zdrowia wzrasta.

Korzyści dla firm ubezpieczeniowych z posiadania w ofercie ubezpieczeń zdrowotnych są nieocenione. Główną przesłanką jest zdobycie nowych

klientów – zarówno indywidualnych osób, jak i klientów korporacyjnych, którzy będą ubezpieczać swoich pracowników. Poszerzenie bazy klientów daje możliwości rozwijania dotychczas sprzedawanych produktów ubezpieczeniowych. Mimo że wydatki w początkowej fazie wdrażania produktu są wysokie, można liczyć, iż ubezpieczenia te dadzą wysoki zwrot zaangażowanego kapitału. Dodatkowo należy liczyć, iż produkty ubezpieczeniowe w przyszłości będą ewaluowały – do typowego ochronnego zakresu ubezpieczenia będą dołączane dodatkowe usługi – jak pakiet assistance medyczny, usługi „spa&wellness” itd. – czyniące ubezpieczenia bardziej atrakcyjnymi i konkurencyjnymi.

### Możliwości systemu Comarch Health Insurance

Zwiększone zapotrzebowanie społeczeństwa na prywatne usługi medyczne wywołało większe zainteresowanie polskich firm ubezpieczeniowych i partnerów medycznych rozwijaniem oferty w zakresie prywatnych ubezpieczeń zdrowotnych. Do obsługi sprzedaży ubezpieczeń zdrowotnych, które różnią się znacznie w obsłudze od pozostałych ubezpieczeń – majątkowych oraz życiowych, niezbędne jest odpowiednie podejście do zarządzania produktem i wsparcie ze strony IT.

Podążając za trendami, polska firma informatyczna Comarch SA – globalny dostawca biznesowych rozwiązań IT – oferuje system do kompleksowej obsługi ubezpieczeń zdrowotnych – Comarch Health Insurance. Podstawowym wyróżnikiem ubezpieczeń zdrowotnych wymagającym uwzględnienia w systemie jest sposób likwidacji szkód. Udział placówek medycznych jako faktycznych likwidatorów szkód, u których ubezpieczeni będą mogli korzystać ze świadczeń medycznych zapewnionych w ubezpieczeniu, wpływa na wiele procesów biznesowych. System umożliwi szybką i bezproblemową komunikację z placówkami medycznymi w celu wymiany informacji niezbędnych do prawidłowego funkcjonowania ubezpieczeń. Komunikacja między towarzystwem ubezpieczeniowym a świadczeniodawcą usług medycznych może odbywać się na kilka sposobów: poprzez zintegrowanie on-line z systemem placówek medycznych albo poprzez portal internetowy lub przez przesyłanie plików płaskich między systemami. W przypadku wymiany informacji poprzez portal internetowy firma ubezpieczeniowa zyskuje dodatkowe narzędzie i możliwość wykorzystania portalu do komunikacji z ubezpieczonymi – pacjentami, którzy mogą on-line sprawdzać dostępność usług medycznych w poszczególnych placówkach, godziny otwarcia placówek, wizyt lekarskich itp. Komunikacja między towarzystwem ubezpieczeniowym a placówką medyczną zapew-

nia, że proces obsługi pacjentów będzie przebiegał poprawnie – placówki medyczne będą posiadały aktualne dane o ubezpieczeniu danego pacjenta, zakresie ubezpieczenia, ewentualnym wykorzystaniu limitów. Towarzystwo ubezpieczeniowe natomiast będzie otrzymywało zwrótną informację o wykorzystaniu ubezpieczenia. Komunikacja między tymi podmiotami umożliwia też rozliczenie za świadczone usługi medyczne.

Kolejną istotną sprawą przy obsłudze ubezpieczeń zdrowotnych jest konieczność zwrócenia się z obszerną bazą danych. Ubezpieczenia zdrowotne wyróżniają się tym od innych produktów ubezpieczeniowych, że wymagają do obsługi dużej liczby rekordów danych. W ramach jednego produktu ubezpieczeniowego może być przyporządkowana duża liczba placówek medycznych, a w ramach każdej z placówek znaczna ilość świadczeń medycznych i odpowiadające im koszty. Nakładając na to jeszcze liczbę ubezpieczonych, która w ramach grupowych ubezpieczeń pracowniczych może sięgać kilkuset lub więcej – tworzy się do obsługi obszerną bazę danych. Budowa systemu Comarch Health Insurance oraz zastosowane rozwiązania są dostosowane do pracy na tak rozbudowanych bazach danych.

System jednocześnie umożliwi efektywne zarządzanie kontaktami do placówek medycznych, rejestrowanie w systemie placówek współpracujących i zarządzających nimi partnerów medycznych, przyporządkowanie do placówek pakietów medycznych wraz z poszczególnymi świadczeniami medycznymi i kosztami, zachowywanie warunków współpracy oraz historii rozliczeń finansowych. Dzięki temu modułowi firma ubezpieczeniowa zyskuje narzędzie do kontrolowania wydatków w podziale na poszczególne sieci medyczne.

System Comarch Health Insurance obejmuje wszystkie procesy potrzebne do kompleksowej obsługi ubezpieczeń zdrowotnych. Pozostałe elementy systemu, które funkcjonują także przy obsłudze innych ubezpieczeń, są dostosowane do specyfiki ubezpieczeń zdrowotnych i obejmują takie funkcjonalności, jak: definiowanie produktów ubezpieczeniowych, kartoteki, zarządzanie wnioskami i polisami, underwriting, rozliczenia, zarządzanie siecią sprzedaży, rezerwy, reasekuracja, raporty i analizy. Dzięki modułowej budowie na życzenie towarzystwa ubezpieczeniowego mogą być wdrożone tylko niektóre części systemu, które zostaną zintegrowane z istniejącym systemem informatycznym klienta. Modułowa budowa umożliwia też etapowe wdrażanie systemu. Comarch Health Insurance oprócz komunikacji z placówkami medycznymi komunikuje się z systemem finansowo-księgowym i systemem bankowym.

#### Przykładowe referencje:

Potwierdzeniem satysfakcji klientów z jakości produktów i usług oferowanych przez Comarch jest szereg referencji uzyskanych przez firmę. Wśród klientów Comarch są tak polskie, jak i zagraniczne podmioty, np.:

- ✔ Towarzystwo Ubezpieczeń Europa,
- ✔ PZU,
- ✔ Commercial Union,
- ✔ UNIQA,
- ✔ ALLIANZ,
- ✔ TUW Pocztove,
- ✔ Towarzystwo Ubezpieczeń na Życie WARTA SA,
- ✔ Fortis Bank,
- ✔ BRE Bank,
- ✔ Bank Pekao,
- ✔ Narodowy Bank Polski,
- ✔ Bank BPH,
- ✔ Bank Zachodni WBK,
- ✔ BP Polska,
- ✔ Procter&Gamble,
- ✔ Nokia Network,
- ✔ Rząd Stanów Zjednoczonych Ameryki Północnej
- ✔ i wiele innych.

## Bezpieczeństwo i jakość

Bogate doświadczenie Comarch SA w przygotowywaniu rozwiązań nie tylko dla towarzystw ubezpieczeniowych, ale także dla banków, licznych instytucji finansowych, jednostek administracji państwowej i podmiotów gospodarczych – gwarantuje kolejnym klientom Comarch wysoki poziom usług z zachowaniem najwyższych standardów bezpieczeństwa co do przesyłu, gromadzenia danych i utrzymania jakości systemu.

Systemy Comarch są realizowane zgodnie z normą ISO 9001:2000, co gwarantuje profesjonalne podejście na etapach produkcji, wdrożenia oraz utrzymania systemu, przy jednoczesnym zapewnieniu wysokiej jakości realizowanych produktów.

Comarch jest zdobywcą licznych wyróżnień i nagród, m.in. został uznany przez Prezydenta RP za Najlepsze Polskie Przedsiębiorstwo w 2000r. oraz przez Światowe Forum Ekonomiczne w Davos w 2000 roku za Pioniera Technologii, czyli firmę, która przyczynia się do poprawy warunków ekonomicznych i gospodarczych na świecie. Comarch otrzymał Nagrodę Gospodarczą Gazety Prawnej „Wehikuł Czasu” w kategorii Firma Technologiczna Roku 2005, został też wyróżniony przez „Gazetę Prawną” i Fortis za innowacyjny produkt w 2007 roku.

## Korzyści biznesowe i operacyjne z wdrożenia Comarch Health Insurance

Wdrożenie systemu Comarch Health Insurance umożliwia kompleksowe i spójne zarządzanie biznesem ubezpieczeniowym. Dodatkowo jego elastyczność pozwala na optymalizację działalności. System pozwala na maksymalne skrócenie czasu wprowadzania nowych produktów ubezpieczeniowych oraz łatwe dostosowanie wdrożonych już produktów w systemie do nowych zmian. Dzięki temu firma ubezpieczeniowa zyskuje w Comarch Health Insurance idealne narzędzie do zarządzania produktami ubezpieczeniowymi, a nie hamulec w rozwijaniu nowych produktów. Atutem systemu jest to, że ewoluuje on wraz z rozwojem firmy ubezpieczeniowej i nowymi wdrożeniami produktów.

Oczywistą korzyścią z automatyzacji obsługi ubezpieczeń zdrowotnych, tak jak z innych procesów, jest oszczędność czasu. W przypadku systemu do obsługi ubezpieczeń zdrowotnych – automatyzacja procesów umożliwia unikanie błędów w zakresie obciążania polis uszkodzeniami i unikanie przestępstw ubezpieczeniowych – a co za tym idzie, redukuje koszty operacyjne w firmie ubezpieczeniowej.

Menadżerowie odnajdą w systemie narzędzia do efektywniejszej kontroli kosztów związanych z likwi-

dadzą szkód. Wymiana informacji z placówkami medycznymi odnośnie szkodowości poszczególnych pakietów medycznych, gromadzenie danych o kosztach usług medycznych i wielowymiarowa analiza szkodowości wspomaga proces decyzyjny w firmie ubezpieczeniowej odnośnie zarządzania produktami ubezpieczeń zdrowotnych.

Wyższą jakość współpracy z placówkami medycznymi i podmiotami trzecimi zapewnia innowacyjność rozwiązań stosowanych przez Comarch. Wpływa to pozytywnie na zadowolenie partnerów medycznych ze współpracy i klientów (ubezpieczonych) z jakości obsługi. Te wszystkie atuty wpływają na zwiększenie atrakcyjności oferowanych ubezpieczeń zdrowotnych, co zwiększa konkurencyjność produktu na rynku ubezpieczeniowym.

## Przyszłość kształtuje się teraz

Wdrażając Comarch Health Insurance, towarzystwo ubezpieczeniowe może być pewne, że nie zatrzyma się w miejscu, kiedy zaimplikuje nowy system, ale że będzie mogło rozwijać produkty ubezpieczeniowe wraz z najnowszymi trendami światowymi. Comarch SA jest otwarty na podłączanie nowoczesnych aplikacji do obsługi ubezpieczeń.

Od kilku lat w Unii Europejskiej propagowany jest program e-zdrowie. Jego głównym założeniem jest wspieranie rozwoju bezpiecznych usług, aplikacji i treści, w oparciu o szeroko dostępną infrastrukturę szerokopasmową. Technologia teleinformatyczna z powodzeniem może być i jest stosowana w zapobieganiu chorobom, w diagnostyce, leczeniu, kontroli oraz w prowadzeniu zdrowego stylu życia.

Szybki rozwój Internetu oraz upowszechnianie się telefonów komórkowych sprzyja między innymi komunikacji między pacjentem a usługodawcami z branży opieki zdrowotnej, przekazywaniu danych pomiędzy poszczególnymi instytucjami oraz bezpośrednim kontaktom zarówno między pacjentami, jak i pracownikami służby zdrowia. Tworzy się internetowe bazy, w których pacjenci mają pod ręką wszelkie informacje nie tylko o placówkach medycznych, lekarzach specjalistach, ale i dane o własnym stanie zdrowia, jak przebyte choroby, alergie, zażywane leki i wyniki badań. Dzięki takiej bazie pacjent może leczyć się w różnych miejscach, po jego akceptacji lekarz otrzyma informacje z systemu, np. wyniki ostatnich badań, i będzie mógł zaktualizować dane o nowe wyniki. Podobną rolę, ale w mniejszym zakresie, mogą spełniać identyfikacyjne karty elektroniczne (lub z chipem), które mogą zawierać ważne informacje, np. grupę krwi, czy przyjmowane leki. Elektroniczne recepty umożliwiłyby kontrolę refundacji leków i rozliczanie aptek z funduszem narodowym.

Operatorzy telefonii opracowują system szybkiego powiadamiania o wypadkach lub nieszczęśliwych zdarzeniach. Usługa zwana mobilnym teledystrybentem opiera się na nadajniku GPS wbudowanym w telefon komórkowy starszej osoby. Jeśli coś jej się przydarzy, nie musi wybierać numeru alarmowego, a wciska jedynie specjalny guzik w obudowie telefonu. W tej samej chwili centrum powiadamiania wie, gdzie znajduje się dana osoba, ma informacje o numerach telefonów najbliższej rodziny i lekarza prowadzącego. Podobnie ma być wdrożony system alarmowy uruchamiany przy poważnych wypadkach drogowych – tzn. w momencie otwarcia się poduszki powietrznej przy zderzeniu samochodu wysyłany będzie sygnał do najbliższej jednostki pomocy o miejscu wypadku oraz rodzaju pojazdu. System będzie można również uruchomić ręcznie. Już w niedługim czasie będzie to obowiązkowym wyposażeniem każdego samochodu w Unii Europejskiej.

Narzędzia klasy e-zdrowie mogą przynieść znaczące korzyści całemu społeczeństwu dzięki poprawie dostępu do opieki zdrowotnej i jej jakości, skoncentrowaniu systemu opieki zdrowotnej na potrzebach pacjenta oraz poprawie skuteczności i wydajności funkcjonowania całego sektora zdrowia.



**Marta Kardela-Trojanowska**

Comarch SA

**Stanowisko:** Konsultant

**Sektor:** Finanse, Bankowość i Ubezpieczenia

# Higiena baz danych

## KRÓTKI ZARYS DEDUPLIKACJI

Bazy i hurtownie danych rozrastają się obecnie w astronomicznym tempie. Duże instytucje dysponują bazami o wielkości rzędu dziesiątek milionów rekordów oraz setek kolumn. W tak dużym zbiorze danych nietrudno jest o błędne wpisy lub powtarzające się wiersze. Aby zapewnić swoim klientom jak najlepszą jakość obsługi oraz zachować jak najwyższą wydajność baz danych, okresowe czyszczenie przechowywanych informacji powoli staje się koniecznością.



**NA** pewno każdy z nas niejednokrotnie spotkał się z sytuacją, gdy w obrębie jednej firmy, z której usług korzystał, wielokrotnie musiał rejestrować swoje dane. Wydanie karty stałego klienta w punkcie sprzedażowym prawie nigdy nie jest równoznaczne z zaistnieniem w całej firmie, która kartę wydała. Próba identyfikacji numerem takiej karty w serwisie technicznym skazana jest w większości przypadków na niepowodzenie, podobnie zresztą jak załatwienie czegokolwiek w obsłudze klienta czy administracji danego przedsiębiorstwa. Jeszcze dobitniejszy przykład podobnej sytuacji pochodzi z obszaru służby zdrowia. Każdy pobyt w szpitalu, zmiana przychodni lub prywatnego usługodawcy to konieczność mozolnego przenoszenia całej dokumentacji związanej z historią pacjenta. Niedopilnowanie fizycznego transferu wiedzy pomiędzy różnymi ośrodkami służby zdrowia to brak jednolitej informacji, która w chwili kryzysowej może okazać się niezbędna dla ratowania życia.

Problem zarysowany w przytoczonych przykładach ma swoje źródło w braku jednolitych systemów informatycznych, które czerpałyby informacje ze wspólnej bazy lub hurtowni danych. W idealnej sytuacji wszystkie szpitale i przychodnie powinny mieć dostęp do pełnej historii swoich pacjentów, a sklep, bank czy ubezpieczyciel powinien udostępnić wszystkim swoim jednostkom możliwość poznania obsługiwanego klienta, tak by przypadkowo nie skierować go do dwóch podobnych akcji marketingowych lub nie zmuszać go do cierpliwego tłumaczenia, jakie usługi ma wykupione oraz z jakiego powodu je reklamuje, po każdym przełączeniu go do kolejnego działu administracyjnego.

To może wydać się w pierwszej chwili nieprawdopodobne, ale wiele firm korzysta często nawet z kilkudziesięciu zupełnie niezależnych baz danych, w których utrzymuje dane swoich klientów. W takiej sytuacji o zamieszanie, nawet w obliczu najmniejszego kryzysu, nie jest trudno.

Kłopoty wynikające z mnogości stosowanych rozwiązań magazynujących dane na linii klient-usługodawca to tylko jedna strona medalu. Kolejnymi problemami są: długi czas potrzebny na zdobycie pełnej informacji o kliencie lub produkcie, koszty związane z utrzymaniem wielu systemów zamiast jednego czy niższe możliwości zaplanowania trafnych i skutecznych akcji marketingowych. Jednym słowem – im większy nieład w przechowywanych informacjach, tym mniejsze szanse na wysoki zysk.

Oczywistym rozwiązaniem wydaje się połączenie baz danych. Jeśli w kilku bazach występuje Jan Kowalski, zamieszkały w Krakowie, przy al. Jana Pawła II, to porównując wiersz po wierszu, znajdziemy go w każdej z baz i połączenie informacji nie powinno stanowić żadnego problemu. Kłopot polega jednak na tym, że w każdej z baz mógł istnieć inny sposób zapisu danych. Przyjrzyjmy się przykładowi przedstawionemu w Tabeli 1, w którym obok siebie zestawiono pięć wierszy pochodzących z różnych baz danych.

Niewątpliwie każdy z pięciu rekordów dotyczy tej samej osoby, jednak każdy wiersz zawiera zupełnie inny zapis, uniemożliwiający połączenia baz na zasadzie „Jeśli wiersz z bazy1 = wiersz z bazy2, to...”. Interesujący jest fakt, że tego typu sytuacji wcale nie trzeba szukać tylko przy procesie łączenia baz danych. Nawet w obrębie jednej bazy danych mogą się zdarzyć tego typu duplikaty wynikające z wielokrotnego rejestrowania tej samej osoby lub produktu. Namacalnym i znanym każdemu przykładem występowania duplikatów w bazie jest wynik zapytania zwracany przez porównywarki cenowe – szczególnie te mniej popularne, które nie zaopatrzyły się jeszcze w stosowne narzędzia do eliminacji duplikatów. Wystarczy w takiej bazie wpisać jakiegoś bardziej złożone zapytanie, by okazało się, że dokładnie ten sam produkt wyświetlany jest wielokrotnie, a każdy odnośnik prowadzi do innego, często jednak zawierającego elementy wspólne, zbioru sklepów.

## Deduplikacja

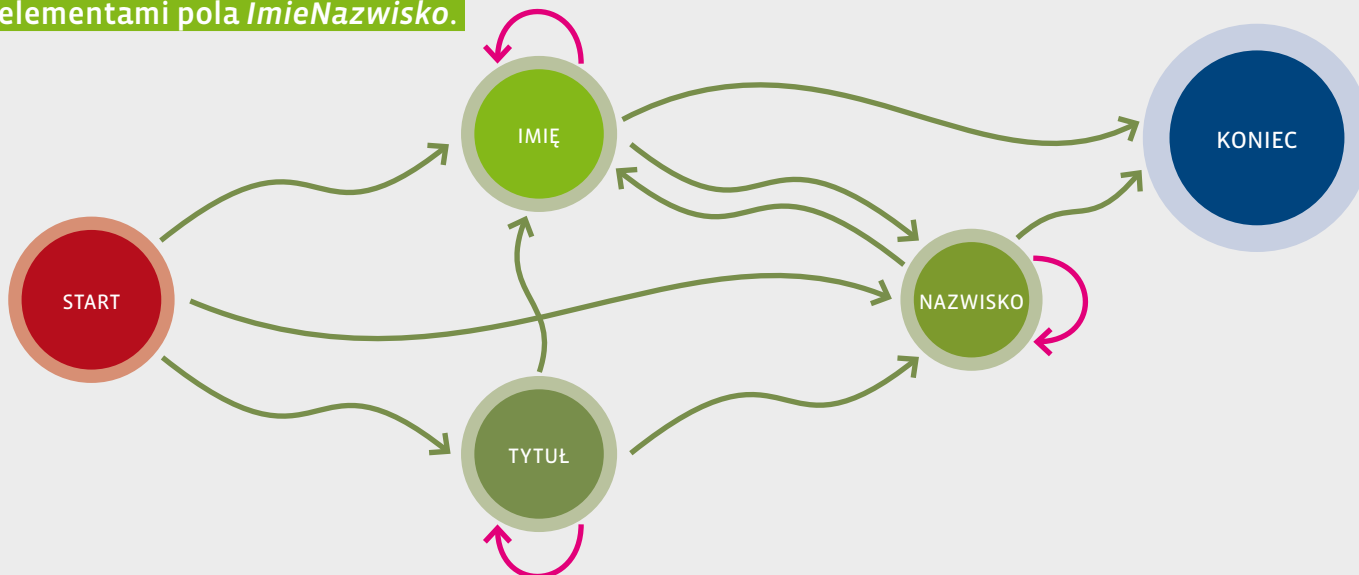
Przy ciągle zwiększającej się infrastrukturze informatycznej, przy liczbie informacji mierzonych w dziesiątkach, setkach GB odkładanych w bazach danych każdego dnia, problem nieporządku i istnienia duplikatów w bazie danych w ostatnich latach nabrał szczególnego znaczenia. Czystość bazy danych bowiem to szybkość jej działania, dokładność i jednoznaczność przechowywanych informacji, niższy koszt jej utrzymania oraz niższa awaryjność. Aby zapewnić odpowiedni poziom jakości danych, coraz częściej stosuje się narzędzia zapewniające wysoką jakość danych, które przeprowadzają deduplikację.

Deduplikacja to bardzo szerokie pojęcie i choć nazwa kojarzy się z usuwaniem duplikatów, to w rzeczywistości rzadko kiedy jest to jej ostatecznym celem. Najczęściej z tym terminem wiążą się operacje ustandaryzowania danych, wyszukiwania potencjalnych duplikatów, a nawet kompresji danych, co dokładniej opisuję poniżej. Historia deduplikacji, jak podają źródła, np. <http://www.enotes.com/public-health-encyclopedia/record-linkage>, sięga aż do 1946 roku, kiedy deduplikacja została użyta w służbie zdrowia. W tym to roku po raz pierwszy pojawił się termin „record linkage”, wprowadzony przez H. L. Dunn – amerykańskiego statystyka, który zdefiniował go w następujący sposób: „Każda osoba tworzy swoją własną księgę życia. Pierwsza strona to urodzenie, ostatnia – śmierć. Record linkage to termin opisujący sposób połączenia pojedynczych stron tej księgi w całość”. Pierwsze zastosowanie deduplikacji znalazła w epidemiologii tuż po wojnie, kiedy łączono napływające z różnych źródeł informacje medyczne w jedną całość, aby w ten sposób móc opisać statystycznie proces życia człowieka oraz śmiertelność powodowaną przez różne choroby i katastrofy. Matematyczne podstawy rozpoznawania duplikatów zostały podane w 1969 roku przez I. P. Fellegiego i A. B. Suntera. Do 2003 roku deduplikacja

**Tabela 1. Przyczyna niskiej jakości informacji zapisanych w bazach danych – brak jednolitego standardu zapisu danych**

Imię	Nazwisko	Miasto	Ulica	Mieszkanie
Jan	Kowalski	Kr	JPII 14	
Jan Kowalski		Kraków	Jana Pawła II	14
Kowalski	Jan	Krakow	al. Jana Pawła 2	14
Janek	Kowalski	Kraków	J. Pawła Drugiego	14
Jan	Kowlski	Kraków	JPII aleja	14

**Rysunek 1. Pierwszy etap procedury parsowania: wyznaczenie możliwych połączeń pomiędzy elementami pola *ImieNazwisko*.**



znajdowała zastosowanie tylko na uczelniach oraz w instytucjach dobra publicznego w USA i krajach Europy Zachodniej. Rok 2003 był rokiem przełomowym, w którym deduplikacja pojawiła się na rynku komercyjnym IT jako narzędzie, a rynek usług deduplikacji wzrósł z poziomu zera dolarów do wartości mierzonych w milionach.

Z punktu widzenia użytkowego deduplikacja jest wieloetapowym procesem, z którym związana jest analiza danych, standaryzacja, indeksowanie, wyszukiwanie duplikatów i na samym końcu właściwa deduplikacja. Oczywiście, w zależności od problemu, nie każdy z tych kroków jest realizowany.

Analiza danych to wstępny proces, mający na celu eliminację z dalszej obróbki rekordów uszkodzonych, zawierających bardzo niestandardowe wpisy (jak wiek = 999 lat), oraz sprawdzenie, czy w bazie nie pojawiają się jakieś oczywiste błędy, jak np. ten sam numer PESEL zapisany wielokrotnie. Krótko mówiąc, do dalszej analizy przeznaczają się tylko te kolumny i rekordy, które wnoszą sensowną informację.

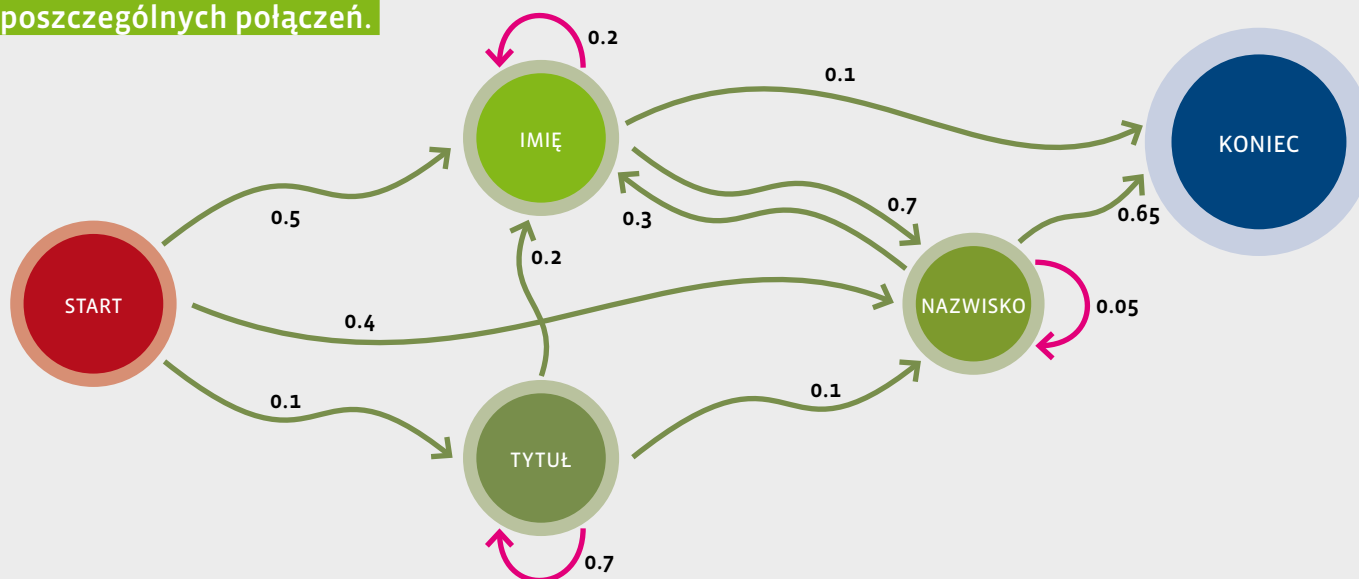
Pod pojęciem standaryzacji kryją się dwa procesy: parsowanie i formatowanie zapisu. W pierwszym odpowiedni algorytm analizuje zawartość pola bazy danych i identyfikuje jej składniki – np. zapis „al. Jana Pawła II 41a” rozbija na trzy znalezione elementy: *Prefixs* (tutaj: „al.”), *NazwaWlasna* (tutaj: „Jana Pawła II”), *Blok* (tutaj: „41a”). Drugi proces obejmuje nadanie ujednoliconej, o identycznej strukturze, postaci każdemu ze sparsowanych pól bazy danych, czyli np. wszystkie numery telefonu zapisuje się w określony sposób (zapisy 1211122233 lub (+4812)

11 12 22 333 23 zastępuje się numerem o postaci 48 (12) 111 222 333), to samo dotyczy dat, które mogą być zapisane na dziesiątki sposobów (12-2-2008 ; 12/08; 2008-02-12; 12/2/08 itd.), a konwertuje się na jeden standard, np. 12-lut-2008. Wszystkim prefiksom nadaje się określoną postać – np. „Ul.”; „ulica”, „ul” zastępuje się „ul.”. Na tym etapie eliminuje się także błędy słownikowe, a zdrobniałe nazwy imion zastępuje się oficjalnie przyjętymi („Grześ”, „Grzesiu”, „Grzesiek” stają się „Grzegorzem”).

Na tym etapie warto wyjaśnić, skąd algorytmy standaryzacji miałyby wiedzieć, że „Grześ” to imię, a „ul.” to prefiks. Informację tę czerpią ze słowników. Gdy analizowana jest kolumna *Imie* to każde jej pole porównywane jest z wartościami słownikowymi. Słowniki natomiast budowane są w taki sposób, by uwzględniać alternatywne możliwości użycia tego samego imienia. Słowniki wykorzystywane są także przy naprawianiu błędów w bazie. Typowym przykładem może być słownik „kod – miasto”. Jeśli potencjalne duplikaty miałyby zapisy postaci „30-072 Kraków” oraz „03-072 Kraków”, to drugi zapis rozpoznany byłby jako błąd, który po porównaniu do pierwszego zapisu dawałby sygnał o znalezieniu duplikatu. Można zadać pytanie, dlaczego nie próbować do kodu 03-072 przypisać miejscowości, która z tym kodem byłaby zgodna. Odpowiedzią jest stwierdzenie, że statystycznie większym prawdopodobieństwem opisane jest przestawieniu dwóch cyfr niż przypadkowa wymiana całego słowa. Tego typu zależności, tj. typowe błędy popełniane przy wprowadzaniu danych, także się bada i uwzględnia w tworzeniu reguł standaryzacyjnych.

Ze względu na złożoność parsowanie doczekało się wielu metod algorytmicznych. Ciągłe jednak dwie z nich wiodą prym. Pierwsza opiera się o reguły logiczne. Dla pola *ImieNazwisko* reguły mogłyby brzmieć „Jeśli pole zawiera jeden wyraz, to sprawdź w słowniku, czy to nazwisko; jeśli dwa wyrazy, to sprawdź, czy pierwszy jest imieniem, jeśli nie to sprawdź, czy jest nazwiskiem; jeśli trzy, to sprawdź, czy pierwsze dwa są imionami lub dwa ostatnie nazwiskami... itd.” Oczywiście, im dłuższa informacja możliwa do zapisania w polu, tym dłuższe reguły. Im dłuższe reguły, tym większa szansa pojawiania się wyjątku od zapisanych reguł, który trzeba opisać... dodatkowymi regułami. Choć jest to dość prosta metoda w implementacji, wymaga doskonałej znajomości sposobu zapisu danych w bazie, a duża liczba reguł czyni tę metodę dość zawiłą i trudną w interpretacji. Druga metoda oparta jest o samouczący się algorytm o nazwie „Ukryte łańcuchy Markova”. Idea jest dość prosta. Zilustruję ją przy pomocy analizy pola *ImieNazwisko*. W pierwszym kroku analityk przegląda te pola w bazie danych lub zastanawia się nad tym, co może się w nich, teoretycznie, znajdować. Przykładowo, możemy spodziewać się zapisu: „mgr inż. Kamil Nowak” lub „Kowalski Grzegorz Piotr” lub „Stefan”, a raczej nie będziemy spodziewać się „Kamil mgr Nowak inż.” Na tej podstawie budowane są diagramy, które pokazują możliwą kolejność elementów takiego pola. Ilustruje to Rysunek 1. Strzałki ukazują możliwe przejście pomiędzy elementami. Strzałka kierująca do tego samego elementu oznacza możliwość jego powtórzenia (np. wiele tytułów lub imion). Dla uproszczenia, w diagramie założono, że jeśli pole się powtarza, to tylko jeden raz.

**Rysunek 2. Drugi etap procedury parsowania: wyznaczanie prawdopodobieństwa realizacji poszczególnych połączeń.**



W drugim kroku algorytm skanuje pola bazy danych, zgodnie z zaproponowanym schematem, i ustala prawdopodobieństwa realizacji odpowiednich połączeń. Przykładowy wynik jego działania przedstawia Rysunek 2.

Liczba 0.7 pomiędzy imieniem i nazwiskiem oznacza, że jeśli w polu napotkane jest imię, to w 70 proc. sytuacji następuje po nim nazwisko. Z diagramu wynika, że najbardziej prawdopodobny zapis, to imię (50 proc.) + nazwisko (70 proc.). Po tej sekwencji zawartość pola najczęściej się kończy (65 proc.).

Gdy reguły parsujące zostaną ustalone, uruchamia się je na pełnej bazie danych. Metoda jest bardzo szybka, bowiem sprawdza kolejne pola zgodnie z najbardziej prawdopodobnymi połączeniami w diagramie. Przykładowo, po imieniu najpierw sprawdzi, czy następnym słowem jest nazwisko (prawdopodobieństwo 70 proc.), a dopiero w razie porażki sprawdzi, czy jest to może drugie imię (prawdopodobieństwo 20 proc.).

Co się jednak stanie, gdy algorytm natrafi na błędny wpis „Szafa dwudrzwiowa składana” lub mocno niestandardowy „Król Zygmunt III Waza”? Możliwości są dwie: albo analityk utworzy dodatkowe możliwe połączenia pomiędzy elementami diagramu, albo wiersze oznaczy jako błędne i nie będzie ich poddawać deduplikacji.

Mając uporządkowaną bazę danych, można rozpocząć jej analizę pod kątem istnienia duplikatów. Tu znowu droga do celu się rozdwaja. Typowym rozwiązaniem jest porównywanie każdego wiersza z każdym, co jednak prowadzi do kwadratowej złożoności obliczeniowej – liczba porównań jest

rzędu liczby wierszy bazy podniesionej do drugiej potęgi. W przypadku średnich baz danych nie stanowi to problemu – komputery są obecnie bardzo szybkie. Gdy jednak należy zmierzyć się z bazą liczącą 100 mln rekordów, sprawa się komplikuje, gdyż potencjalnie oznacza to rząd  $10^{16}$  (10 milionów miliardów) porównań. Bardziej zaawansowane, obecnie rozwijane algorytmy próbują więc przed właściwym poszukiwaniem duplikatów opisać wiersze przy pomocy liczb (indeksów), które obrazują to, co w wierszu się znajduje. Następnie porównywana jest zawartość tylko tych wierszy, których indeksy są zbliżone. Metody te nie gwarantują jednak 100 proc. poprawności. Czasami zdarza się tak, że choć indeksy mają skrajnie różną wartość, wiersze są swoimi duplikatami. Jest to jednak alternatywa, która pozwala nam wybrać oszczędność czasu nad wysoką dokładnością.

Porównywanie wierszy i określanie prawdopodobieństwa tego, że są to duplikaty, to kolejny zestaw wielu algorytmów, które lepiej lub gorzej sprawdzają się w różnych sytuacjach. Krótko opiszę jeden z nich.

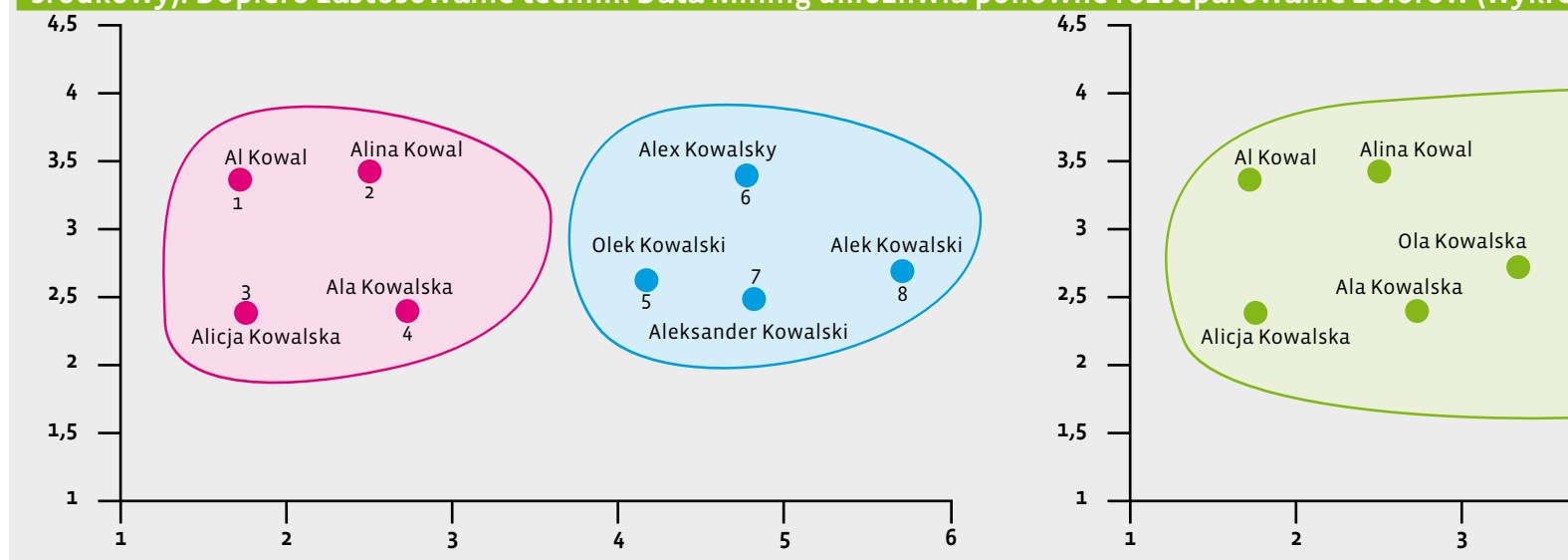
Metoda jest bardzo intuicyjna i polega na prostym założeniu, że im więcej porównywanych pól się zgadza ze sobą, tym większa jest szansa, że wiersze są duplikatami. Jeśli więc z 7 pól 6 jest identycznych, a jedno różne, to raczej jest to duplikat, jeśli tylko dwa, to raczej nie. Ponieważ naiwność tej metody jest dość oczywista, powstały jej modyfikacje uwzględniające dodatkowo pewne zależności statystyczne. Na przykład: analityk może wylosować próbkę 300 wierszy, ocenić, które są duplikatami, sprawdzić, które pola nie są jednoznaczne,

i tym polom przypisać wagi wskazujące, jak często dane pole powodowało niejednoznaczność przy identyfikacji duplikatu. Inne zależności statystyczne mogą uwzględniać fakt częstotliwości występowania pewnych słów w polu. Np. jeśli znajdziemy bardzo rzadko spotykane nazwisko „Kwalski” to jest znacznie większe prawdopodobieństwo, że chodzi o „Kowalski”, niż w sytuacji, gdy porównujemy nazwiska typu „Kwieć” i „Kwiat”.

Oczywiście istnieją także metody działające znacznie bardziej automatycznie. Oparte są one o tzw. miary odległości, które oceniają, jak bardzo podobne są do siebie poszczególne pola w kolumnach. Przy takiej mierze „Kwalski” jest bardzo podobny do „Kowalski”, bo różni się tylko jednym znakiem na 8, zaś „Kwieć” i „Kwiat” aż 2 na 5.

Znalezione pary potencjalnych duplikatów to dopiero pierwszy krok przy ich wyszukiwaniu. Kolejnym krokiem jest próba automatycznego znalezienia fałszywych duplikatów. Takie powstają, gdy w kilku parach potencjalnych duplikatów znajdują się wiersze, które wykazują podobieństwo także pomiędzy tymi parami. Oto przykład: „Bąk” i „Sęk” – oba słowa to polskie nazwiska, więc raczej o duplikatach nie ma mowy. Ale jeśli w bazie znajdzie się nazwisko „Bęk”, to wszystkie algorytmy uznają, że jest ono podobne tak do „Bąk” (wymiana „ę” na „ą”), jak i do „Sęk” (wymiana „B” na „S”). W ten sposób te trzy słowa zostaną zgrupowane do jednej grupy potencjalnych duplikatów i „Bąk” może stać się „Sękiem” lub na odwrót. Rozwiązania tego typu problemów leżą w metodach Data Mining, a ich zastosowanie może zobrazować następujący przykład. Załóżmy, że to, czy 2 wiersze są duplika-

**Schemat 1. Wpływ pojedynczego rekordu na błędne rozpoznanie duplikatów. Tutaj „Ola Kowalska” powoduje (środkowy). Dopiero zastosowanie technik Data Mining umożliwia ponowne rozseparowanie zbiorów (wykreślenie).**



tami, oceniamy na podstawie tylko dwóch kolumn: *Imie* i *Nazwisko*. Nie wchodząc w szczegóły techniczne, załóżmy dalej, że każdemu polu przypisujemy pewną wartość liczbową, która to pole charakteryzuje, oraz że jeśli dwie liczby z kolejnych pól są sobie bliskie, to oba pola z dużym prawdopodobieństwem są duplikatami. Przyjrzyjmy się sytuacji zobrazowanej na Schemacie 1, gdzie na dwuwymiarowym wykresie na osi Y mamy odłożone wartości liczbowe opisujące pola z kolumny *Nazwisko*, a na osi X znajdują się wartości odnoszące się do pól kolumny *Imie*. Widać wyraźnie, że punkty 1, 2, 3, 4 leżą bardzo blisko siebie. Są to potencjalne duplikaty. To samo można powiedzieć o punktach 5, 6, 7 i 8, które jednak znajdują się w znacznej odległości od pierwszej grupy punktów. Nad punktami umieszczone są możliwe wartości czyniące z nich potencjalne duplikaty. Na rysunku widać dwie duże grupy potencjalnych duplikatów.

Co się jednak stanie, gdy w bazie pojawi się wpis „Ola Kowalska”? Jest to imię bliskie zarówno imieniu „Ala”, jak i „Olek”. „Ola” wprowadzi pomost spajający obie grupy i w ten sposób utworzy się grupa dziewięciu potencjalnych duplikatów, z których jednak większość to fałszywe duplikaty.

Z tego typu problemami nowoczesne programy deduplikujące radzą sobie poprzez wykonanie tzw. segmentacji lub klastrowania przy pomocy metod Data Mining. Taki algorytm wykryje „przewężenie” pomiędzy grupami i utrzyma je jako niezależne dwie grupy potencjalnych duplikatów. Co się jednak stanie w takim wypadku z obiektem „Ola”? Zostanie włączony do tego zbioru, do którego jest mu bliżej.

Mając już wykryte potencjalne duplikaty, należy zastanowić się, co możemy z nimi zrobić. Możliwości są dwie:

- a) możemy zaufać automatowi i pozwolić mu połączyć je (i w ten sposób dokonać właściwej deduplikacji),
- b) możemy przesłać ich listę do osoby odpowiedzialnej za weryfikację poprawności deduplikacji, która ostatecznie decyduje, które wiersze należy uznać za duplikaty, a które nie.

W praktyce realizowany jest najczęściej punkt drugi. Dane przechowywane w bazach są zbyt cenne, aby pozwolić na ich przypadkową, nieprzewidywalną modyfikację.

### Obszary zastosowań deduplikacji

Obecnie deduplikacja to nie tylko trend czy ciekawostka techniczna dostępna jedynie dla największych firm, lubiących wdrażać zaawansowane i nowe technologie. Deduplikacja powoli staje się koniecznością, a zakres jej zastosowań jest szeroki:

- ▶ **Budowa hurtowni danych.** Hurtownia danych powstaje na podstawie danych zgromadzonych w wielu różnych źródłach. Deduplikacja danych jest w tym przypadku wręcz niezbędna, jeśli od samego początku nie chce się wprowadzać do hurtowni wielokrotnie tych samych rekordów zapisanych w różnych bazach. Rekordy porównywane są pomiędzy różnymi bazami danych, a do hurtowni trafiają te informacje, które są najpełniejsze i najaktualniejsze.
- ▶ **Implementacja systemów integracyjnych.** Nowoczesne systemy nie muszą mieć dostępu do hurtowni danych, by odpowiednio zarządzać infor-

macjami pochodzącymi z różnych baz danych. W takim wypadku deduplikacja służy tylko oznaczeniu rekordów odnoszących się do tego samego obiektu (np. klienta lub produktu). Gdy system wywołuje kartotekę klienta, jednocześnie otwiera informacje pochodzące z bazy personalnej, bazy sprzedażowej, bazy serwisu, administracyjnej itd.

#### ▶ Okresowa deduplikacja bazy / hurtowni danych.

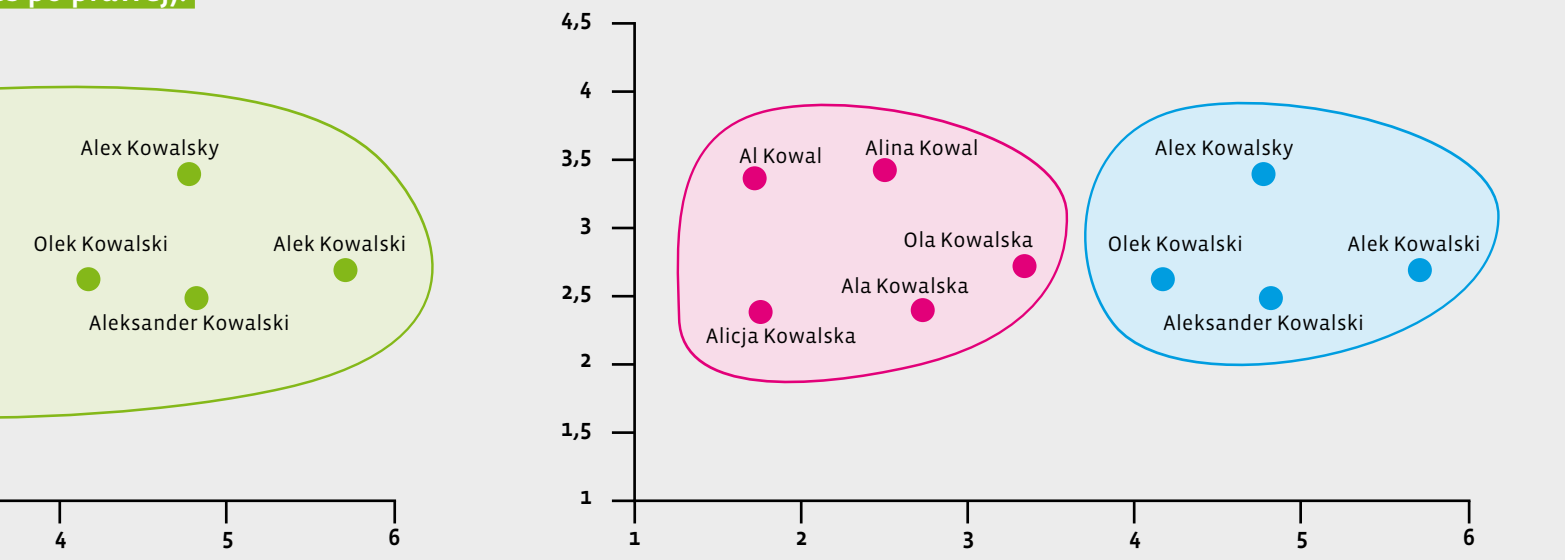
W każdej bazie danych, niezależnie od jej stanu początkowego, po pewnym czasie pojawiają się duplikaty. Aby zapewnić jej maksymalną wydajność, okresowo przeprowadza się na niej wyszukiwanie i eliminację duplikatów.

#### ▶ Deduplikacja „w locie”.

Jest to najbardziej złożony proces deduplikacji. Stosujemy ją, gdy chcemy zapobiec przypadkowemu założeniu przez konsultanta nowego konta dla klienta, który jest już w bazie zarejestrowany, lub uniknąć tego, by do bazy produktowej zostały wielokrotnie wprowadzone te same pozycje. Wyobraźmy sobie sytuację, gdy konsultant podczas obsługi klienta zamiast „Jan Kowalski”, wpisałby przypadkowo „Jan Kwalski”. Zwykle system zgłosiłby, że klient nie istnieje, jednak system wyposażony w przebiegający w tle proces deduplikacji, bez trudu odnajduje powiązanie prawidłowego rekordu z danymi wpisanymi przez konsultanta. Konsultant jest wtedy informowany o prawdopodobnej pomyłce i wskazywane są mu prawdopodobne, prawidłowe nazwiska.

- ▶ **Kompresja danych.** Wyobraźmy sobie sytuację, w której do 5 znajomych wysyłamy email z załącznikiem o wielkości 10MB, a każda z tych osób przesyła ten email średnio do trzech kolejnych znajo-

e połączenie dwóch różnych (wykres po lewej) obiektów w jeden (wykres po prawej).



mych. W ten sposób ten sam plik zapisywany jest w bazie emailowej  $5 \times 3 + 5 + 1 = 21$ -krotnie! Proces deduplikacji wyszukuje tego typu kopie, w bazie pozostawia tylko jedną wersję pliku, a do reszty prowadzi jedynie odnośniki. Tego typu kompresja daje nawet kilkunastokrotne zmniejszenie zajmowanej przez rekordy objętości (w naszym przykładzie rzędu 1:21).

▶ **Przygotowanie danych pod analizę.** Ta sama informacja wielokrotnie zapisana będzie wpływać negatywnie na wyniki wszelkiego typu analiz liczbowych przeprowadzanych na kolumnach bazy. Nieprawdziwa będzie liczba klientów czy produktów, błędnie będą obliczane średnie, wszelkiego typu wskaźniki. Także modele prognostyczne nie będą mogły być precyzyjne, jeśli dane na wejściu nie będą prawidłowo reprezentować realnego, unikalnego zbioru rekordów bazy. Z tego powodu deduplikacja jest jedną z wstępnych metod selekcji zbioru rekordów przeznaczonych do analiz typu Data Mining.

## Podsumowanie

Rynek deduplikacji gwałtownie rośnie. Przy ciągle powiększających się objętościach hurtowni i baz danych utrzymanie porządku w nich staje się niezbędne dla szybkiej, wydajnej i bezawaryjnej pracy. Także zadowolenie klientów ma ogromne znaczenie. Klient wielokrotnie poddany tym samym zabiegom marketingowym lub zmuszony do wielokrotnej identyfikacji w kolejnych punktach tej samej firmy nie pozostanie długo lojalnym klientem. Ponieważ pozyskanie klientów jest znacznie bardziej kosztowne niż ich utrzymanie, deduplikacja staje się koniecznością i standardową procedurą czyszczącą bazy danych.

Wartość rynku usług deduplikacji jest ogromna. W 2003 roku deduplikacja była jedynie ciekawostką i jak podaje artykuł <http://www.networld.pl/news/128533.html>, obroty pieniężne na tym rynku były równe dokładnie zero. Rok później rozpoczęła się rewolucja trwająca do dziś. W 2006 roku obrót osiągnął wartość 100 mln \$, w 2007 miał zbliżyć

się do 300 mln \$, by w 2009, zgodnie z prognozą, przekroczyć 1 mld \$!

Na rynku polskim nie wyczuwa się jeszcze dużej potrzeby czyszczenia baz danych, a do deduplikacji duże instytucje finansowe podchodzą z dużą ostrożnością. Wychodząc jednak naprzeciw potrzebom rynku, moduł analityczny systemu Comarch CRM został wyposażony w stosowny zestaw algorytmów do wyszukiwania wierszy potencjalnie mogących być duplikatami. Krótki jego opis znajduje się w ramce.



**Bartłomiej Kozakowski**

Comarch SA

**Stanowisko:** aCRM Business Solution Manager

**Sektor:** Finanse, Bankowość i Ubezpieczenia

**Info:** W Comarch SA zajmuje się rozwojem platformy aCRM

## Moduły oraz techniki Data Mining implementowane w Comarch aCRM

Comarch aCRM to kompleksowe rozwiązanie CRM, którego centrum stanowi Moduł Decyzyjny zarządzający wymianą informacji pomiędzy modułami: Analitycznym, Sales Management, Campaign Management, Loyalty Management, Contact Center. Źródło danych dla aplikacji stanowi hurtownia danych tworzona z wielu małych, lokalnych baz danych przez wyposażony w narzędzia deduplikacyjne moduł DPETL.

### Algorytmy:

- ▶ Grupujące: k-mean, k-medoids, DBSCAN, PAM, BIRCH.
- ▶ Klasyfikujące: samouczące się algorytmy: CART, CHAID, C4.5 oraz sieci neuronowe.
- ▶ Techniki uzupełniające: detekcja duplikatów, wartości odstających, wypełnianie brakujących wartości, regresja liniowa i logistyczna, statystyka opisowa, testy statystyczne i wiele innych.
- ▶ Proces przygotowywania modeli jest prowadzony i sterowany algorytmem CRISP.

# Ocean jest Agile

**REWOLUCYJNE ROZWIĄZANIA W POŁĄCZENIU Z EWOLUCJĄ ZAŁOŻEŃ: OCEAN W ADMINISTRACJI PUBLICZNEJ**

Ocean to nieustanny rozwój. Rozwiązanie średniego kalibru w ciągu roku przerodziło się w rodzinę produktów, których wspólnym celem jest realizacja głównego założenia: Adresacja Biznesowych Potrzeb Klienta, w skrócie – Agile.

**NA** powstała w centrum Błażeja Chodarczewicza platformę składają się obecnie cztery produkty. Każdy z nich odpowiedzialny jest za zaspokajanie potrzeb organizacji na różnych, wzajemnie powiązanych polach:

- ▶ **Ocean Workflow** – system elektronicznego obiegu dokumentów – zarządzanie dokumentami i przepływem pracy,
- ▶ **Ocean Portal** – system zarządzania i publikacji treści (CMS) wraz z Elektroniczną Skrzynką Podawczą oraz Biuletynem Informacji Publicznej,
- ▶ **Ocean PKI** – system obsługi infrastruktury PKI, w tym Centrum Certyfikacji oraz moduły do składania i weryfikacji podpisów elektronicznych,
- ▶ **Ocean CDAR&GenRap** – system analityczny i raportujący.

Funkcjonalne dopełnianie się elementów platformy Ocean dodatkowo wzmacnia końcowy rezultat.

## O jakich potrzebach mowa?

Specyfika sektora publicznego pozwala określić podstawowe wymagania wobec systemów informatycznych: system winien być zgodny z prawem i tani... a także ładny, funkcjonalny, zorientowany na usługi – zgodnie z SOA, zorientowany na użytkownika – zgodnie z Web2.0, skalowalny, dynamiczny, wyposażony w kreatory, modelery, repozytoria i naprawdę tani... Dopiero spełnienie tych wszystkich oczekiwań pozwoli pomyśleć... rozpoznać wdrożenie.

## Skąd takie potrzeby?

Potrzeby biznesowe w sektorze publicznym to wypadkowa wielu czynników: technologicznych, marketingowych, politycznych. Decydujące z tych potrzeb kreują następujący aktorzy:

- ▶ **Ustawodawca** – określając szczegółowo ramy i zakres działań instytucji, pozostawia margines na interpretację. Narzucając obowiązki, oczekuje ich realizacji, ale w sposób odpowiadający realiom urzędu.
- ▶ **Urzędnik** – ten sam, który zgodnie z wynikami badań poświęca jedną trzecią dnia na wyszukiwanie informacji, weryfikację aktualności danych wprowadzanych do trzech różnych systemów dziedzinowych, oczekujący, iż system informatyczny rzeczywiście ułatwi pracę, a nie przysporzy kolejnych obowiązków.
- ▶ **Petent** – obywatel odpowiedzialny za dynamiczny rozwój społeczeństwa informacyjnego. Kolejki, wielokrotne wizyty w urzędzie, sterty zapisanych bądź zadrukowanych podań, wniosków, załączników – taki stereotyp urzędu nadal pokutuje wśród obywateli. Wypełnienie dziesiątek stron

formularzy, wędrowki od okienka, do okienka, oczekiwanie, oczekiwania... Nowoczesne Społeczeństwo Informacyjne marzy o Nowoczesnym Urzędzie!

## Jest potrzeba, jest odpowiedź. Jest Ocean.

Urząd, zarówno ten realny, jak i ten cyfrowy, oparty jest o procedury – formalne i nieformalne – podzielone na etapy, z produktami w postaci dokumentów i decyzji. W większości jednostek administracji publicznej można zidentyfikować od kilkudziesięciu do kilkuset procesów, których przebieg (wynikający z KPA i Instrukcji Kancelaryjnej, choć zawsze wzbogacony o czynniki właściwe danej instytucji) utrwalał jest... w głowach pracowników. Urzędnik wie, komu powinien przekazać dokumenty, wie, w jaki sposób je wypełnić i ile pieczęci nada mu wartość urzędową. O ile brak szczegółowej kodyfikacji tej wiedzy oraz zarządzanie procesami stanowi sporą trudność, to problemy powstają już na bardziej podstawowym poziomie. Nawet najlepiej ugruntowana procedura nie ustrzeże się przed kwestiami wynikającymi z natury i sposobu przetwarzania papierowych dokumentów.

**Podstawowym** źródłem komplikacji jest tu już sam dokument. Owo pismo – sztuk jeden, które stanowi podstawę do wszczęcia sprawy i pieczołowitego procesowania go z biurka na biurko. Pismo to może być wielokrotnie kserowane (by przekazać je do wglądu uprawnionym osobom), przetrzymywane pod stertą innych pism, poszukiwane (w segregatorach/ teczkach/ zeszytach ksiąg podawczych), a nawet gubione. Papierowa postać dokumentu sprawia, że trudno zapanować nad kolejnymi adnotacjami, zmianami dodawanymi ad hoc czy wersjami dokumentu. Dlatego tak istotne jest stworzenie **wersji elektronicznej**. Wówczas taki cyfrowy dokument, zarejestrowany w kancelarii lub sekretariacie systemu Workflow, cały proces przechodzi wirtualnie:

- ▶ zadekretowany dokument, zeskanowany, zaopatrzone w **metrykę**, załączniki (często uprzednio poddane obróbce w module OCR), powiązany jest ze sprawą, przypisywany do definiowalnych rejestrów i kategorii archiwalnej,
- ▶ przeszukiwany pełnotekstowo i wersjonowany,
- ▶ zaopatrzone w komentarze może zostać asygnowany do dowolnie zdefiniowanych klasyfikacji i teczek.

Możliwości wykorzystania i przetwarzania dokumentu w Ocean Workflow ograniczone są tylko **wyobraźnią i uwarunkowaniami prawnymi**.

**Drugim** źródłem perturbacji w procesach jest... człowiek. To urzędnik poświęcający sporą część czasu na wyszukiwanie aktualnych wersji dokumentu,

**Agile (Zwinny)** – nawiązuje do Agile Software Development – technik i metodologii wytwarzania oprogramowania, stawiających nacisk na bezpośrednią komunikację z klientem, iteracyjny rozwój oprogramowania i realizację projektów, a przede wszystkim ciągłą i aktywną adaptację do zmieniających się warunków.

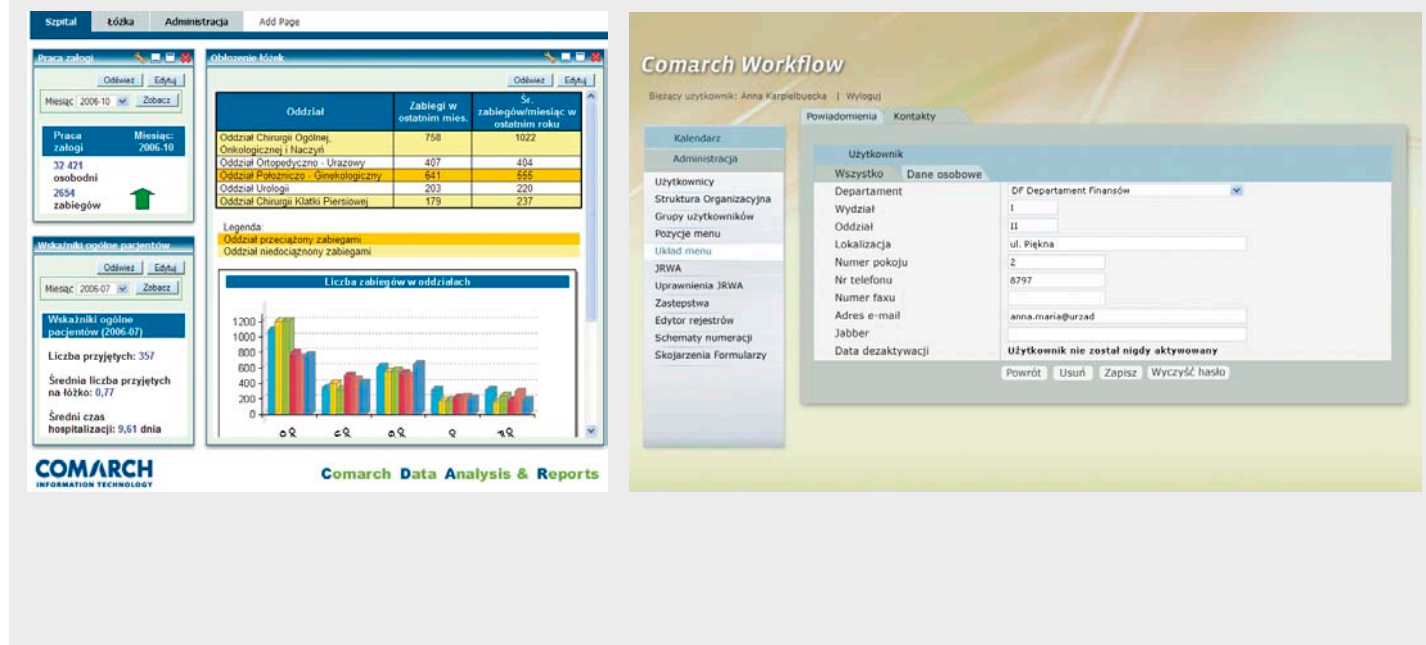
weryfikację, przekazywanie do dalszego procesowania. Urzędnik na zastępstwie, przejmujący rozpoczęte sprawy, urzędnik w delegacji, na którego powrót czeka wysoki i nieuporządkowany stos dokumentów. System Ocean Workflow wychodzi naprzeciw i tym zagadnieniem:

- ▶ możliwość definiowania dowolnej struktury organizacyjnej,
  - ▶ przydzielanie ról i autoryzację uprawnień do spraw, procesów, dokumentów,
  - ▶ definiowanie zastępstw, określanie priorytetów zadań i udostępnienie narzędzi kontroli terminowości wykonania,
  - ▶ mechanizmy pracy grupowej (praca grupowa nad dokumentem, kalendarze prywatne i publiczne, powiadomienia, IM czy konta pocztowe)
- to tylko nieliczne z funkcji Ocean Workflow, których głównym celem jest – **ułatwianie**.

**Trzecią** determinantą jest... przyzwyczajenie. A przyzwyczajenie to druga natura. Wdrożenie systemu, który nie będzie **komplementarny** wobec przyzwyczajenia pracowników, z góry spisane jest na niepowodzenie. Dlatego za niewątpliwą zaletę Platformy Ocean należy uznać fakt, iż w systemie odwzorowywane są rzeczywiste procedury jednostki, a możliwości konfiguracyjne odświeżają pojęcie **elastycznej aplikacji**. To system dostosowywany jest do potrzeb urzędu, a nie urząd do konstrukcji gotowego rozwiązania. Przy czym przez dostosowanie rozumiem cały kilkietapowy proces:

- ▶ szczegółową analizę, w czasie której identyfikowane i porządkowane są **formalne i nieformalne** procedury obowiązujące w urzędzie,
- ▶ konfigurację aplikacji zgodnie z potrzebami klienta,
- ▶ definiowanie struktury organizacyjnej, ról, uprawnień, rejestrów, klasyfikacji, a więc elementów opisujących cały entourage instytucji,
- ▶ modelowanie właściwych procesów – następujące po zdefiniowaniu reguł i możliwych wyjątków (co ciekawe czasem liczniejszych od samych

## Rysunek 1. Przykładowe realizacje



reguł – stąd zapewne najpopularniejszym rodzajem procedury w urzędach jest procedura ogólna umożliwiająca procesowanie ad hoc).

Usprawnienie pracy urzędu to krok w przyszłość, lecz właściwą istotą i celem jest przecież ułatwienie realizacji spraw obywatelom. A skoro wirtualizacji uległy centra rozrywki, sklepy, poczta, a nawet banki, czyż nie przyszła pora na Cyfrowy Urząd? Otóż bez wątpienia tak.

### E-Urząd

Możliwość przedłużenia umowy dzierżawy czy złożenia wniosku o wpis do ewidencji działalności gospodarczej w przyjaznych warunkach własnego biura lub salonu (z dowolnego miejsca na ziemi i o dowolnej porze!), późniejsze zapoznanie się z przebiegiem sprawy, czy odbiór decyzji on-line to solidny sprawdzian rozwoju społeczeństwa informacyjnego. Rewolucyjne? Skądże. Comarch skutecznie wdrożył rozwiązanie Ocean Portal w Urzędzie Miasta Ciechanowa, w Śląskim Urzędzie Wojewódzkim i Urzędzie Marszałkowskim Województwa Wielkopolskiego.

Implementacja Elektronicznej Skrzynki Podawczej w Ocean Portal, a także graficzny Edytor Formularzy – podstawowe funkcjonalności Cyfrowego Urzędu – zaprojektowane zostały tak, by **maksymalnie usprawnić** tworzenie i publikację kolejnych procedur **on-line**. Możliwość wglądu w historię sprawy, przechowywanie całej korespondencji z urzędem

w profilu użytkownika (w tym dokumenty Urzędowego Poświadczenia Odbioru UPP/UPD, decyzje, załączniki) dają petentom wygodę, a urzędowi renomę otwartej i przyjaznej instytucji.

Cyfrowy Urząd jest kluczowym modulem Ocean Portal – kolejnym równie ważnym jest Biuletyn Informacji Publicznej, pozwalający przede wszystkim realizować ustawowy obowiązek upublicznienia informacji. W module zapewniona jest dostępność gotowych do wykorzystania predefiniowanych szablonów oraz odpowiednia obsługa standardów bezpieczeństwa. BIP w Ocean pozwala tworzyć biuletyny jednostek podległych, zachowując spójną i estetyczną formę dla wszystkich, a integracja z systemem Ocean Workflow pozwala publikować na stronach dane bezpośrednio z systemu elektronicznego obiegu dokumentów (zestawienia, raporty, zawartość rejestrów).

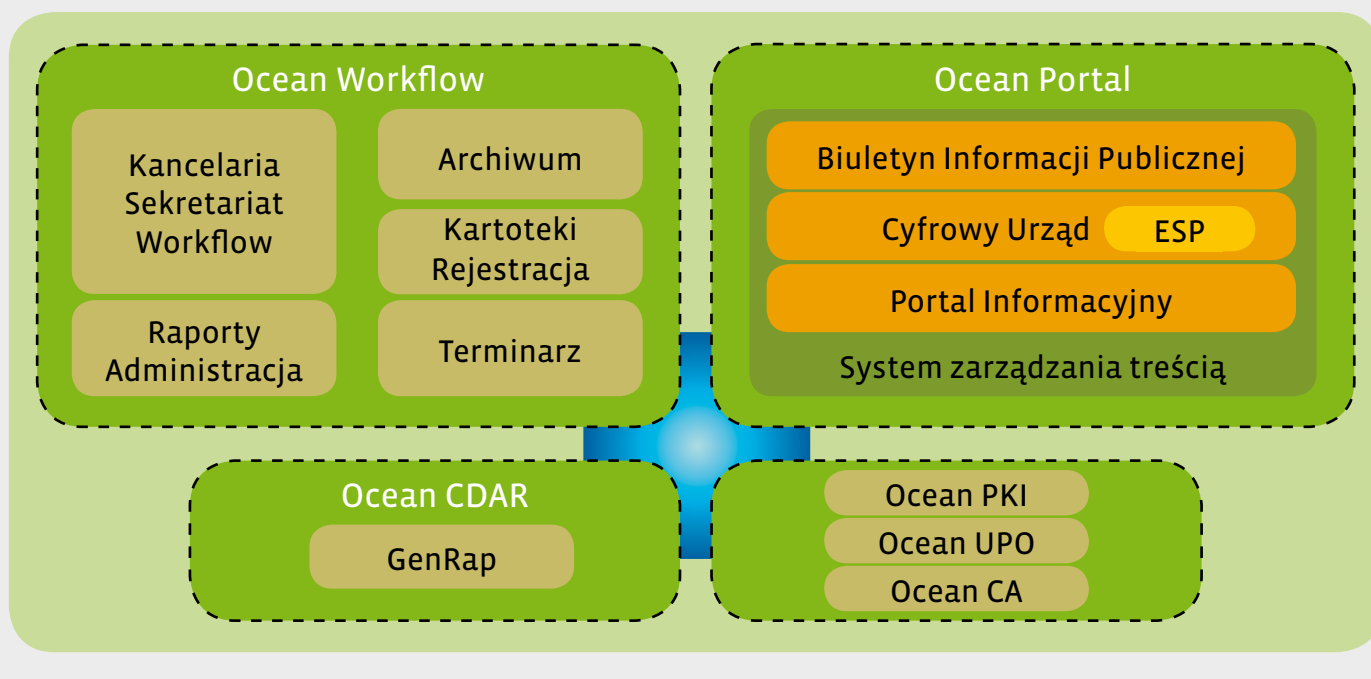
O ile zasadniczym celem modułów BIP i Cyfrowego Urzędu jest realizacja ustawowych obowiązków, o tyle słowami kluczowymi dla modułu Serwisów Informacyjnych w Portalu są: ‘Promocja’, ‘Wizerunek’, ‘Informacja’. Prawdą jest, że ‘każdemu przysługuje prawo dostępu do informacji publicznej’, ale prawdą jest też, że obecnie w poszukiwaniu dowolnej informacji kierujemy się nie w stronę bibliotek, kiosków z gazetami czy słupów ogłoszeniowych, ale przed ekran komputera. Przeglądarka internetowa stanowi dla wielu okno na świat, więc dlaczego nie wykorzystać tego faktu? Dlaczego nie przenieść informacji promujących region i urząd

z gazetki ściennej na portal urzędu? Dlaczego nie nagłaśniać chlubnych inicjatyw społecznych (posezonowa akcja sprzątanía świata, szpital przyjazny matce)? Wzbogacone o galerie fotograficzne, fora i giełdy ogłoszeń Serwisy Informacyjne Ocean Portal są platformą, która pomaga budować społeczność wokół zagadnień związanych z życiem regionu i jednocześnie znacznie poprawia wizerunek instytucji. Przyjazny i intuicyjny system zarządzania treścią portalu (CMS) sprawia, że za utrzymanie i aktualizację treści odpowiedzialne mogą być osoby merytoryczne – te, które mają najgłębszą wiedzę w danej dziedzinie, lecz niechętnie patrzą na narzędzia bardziej skomplikowane niż pakiety oprogramowania biurowego typu Open Office czy MS Office (nota bene Ocean Portal pozwala na bezpośrednie wklejanie sformatowanych treści z edytorów tekstu, zachowując przy tym zgodność z formatem dokumentu xhtml, a także znacząco zmniejszając rozmiar kopiowanych treści).

### „Czy mogę prosić o autograf?”

I kiedy już zatroszczymy się o wygodę pracownika, dostarczając mu Ocean Workflow, gdy zadbamy o wizerunek instytucji, wdrażając Ocean Portal, warto postawić kropkę nad i, którą jest implementacja infrastruktury podpisu elektronicznego. Ocean PKI został stworzony do obsługi certyfikatu elektronicznego. Komponenty systemu pozwalają na składanie i weryfikację podpisu kwalifikowanego oraz niekwalifikowanego na wnioskach elektronicznych

Rysunek 2.



przesyłanych przez petentów z Cyfrowego Urzędu, a także w Ocean Workflow na dokumentach i decyzjach podpisywanych przez pracowników. System umożliwia generację Urzędowych Poświadczeń Odbioru (UPP/UPD) przy współpracy z modułem HSM oraz na znakowanie czasem. Zapewniona jest zgodność z wymaganiami ustawowymi Polski i dyrektywami unijnymi. Dodatkowo ważnym i trudnym do przecenienia elementem systemu Ocean PKI jest Centrum Certyfikacji. Dzięki umocowniom prawnym urząd przy wykorzystaniu Centrum Certyfikacji może wydawać obywatelom podpisy niekwalifikowane, które następnie mogą zostać wykorzystane do podpisania wniosku w Cyfrowym Urzędzie. Obywatel skorzysta z niego, załatwiając sprawy on-line jedynie w danej instytucji, ale i tak jest to ogromne ułatwienie (biorąc pod uwagę koszty podpisu kwalifikowanego). Innym, równie ważnym (jeśli nie ważniejszym) sposobem wykorzystania jest możliwość wydawania certyfikatów niekwalifikowanych pracownikom. Przykładowo: wdrożenie w Urzędzie Marszałkowskim Województwa Wielkopolskiego dla 1000 użytkowników objęło również Centrum Certyfikacji. Jedynie kilka procent pracowników UMWW posiada podpisy kwalifikowane, pozostali zostaną docelowo wyposażeni w certyfikaty niekwalifikowane. Dzięki temu będą mogli parafować dokumenty, potwierdzając ich integralność i niezaprzeczalność. Praktyczne rozwiązanie, które pozwoli zaoszczędzić naprawdę spore sumy.

### Dobrze, a co na to dyrektor?

Pani dyrektor zapewne oczekuje terminowego wykonywania powierzonych zadań. Chciałaby również, aby systemy informatyczne wspomogły ją w podejmowaniu decyzji, dostarczając informacji z rozlicznych systemów wewnętrznych. Na koniec zaś – zaplanować tydzień pracy, a informację o delegacji umieścić w ogólnodostępnym terminarzu.

Ocean Workflow w połączeniu z narzędziami raportującymi Ocean GenRap & CDAR (Comarch Data Analysis & Reports) dostarcza intuicyjnych instrumentów do kontroli pracowników. Terminowość wykonywanych zadań, prywatne i publiczne terminarze, raporty wszelkiej maści pozwalają nadzorować procesy w urzędzie. Niewątpliwą zaletą Ocean GenRap jest nie tylko możliwość zbierania i analizowania danych z systemów znajdujących się w instytucji, ale również prezentacja ich w różnych formatach i widokach. Co ciekawe, autorami najbardziej skomplikowanych raportów pobierających informacje z baz danych (przykładowo Systemu Obiegu Dokumentów czy ERP) również mogą być osoby merytoryczne, nieposiadające żadnej wiedzy dotyczącej tworzenia zapytań SQL. Każdy, kto poradził sobie z pakietem biurowym, bez problemów 'wyklika' (metodą drag'n'drop) definicję raportu.

### Co dalej?

Najprostsza odpowiedź – rozwój. Wyzwanie zostało podjęte. Twórcy Ocean rozbudowują platformę o nowe podsystemy, a podsystemy wzbogacają o kolejne funkcjonalności. Szczegółowe informacje o produktach można uzyskać na stronach <http://ocean.comarch.pl>



**Julia Domżańska**

Comarch SA


**Stanowisko:** Product Manager Ocean Portal & Workflow

**Sektor:** Administracja Publiczna, Utilities i Samorządy (APUS)

**Info:** W Comarch SA zajmuje się rozwiązaniami portalowymi w administracji i jednostkach użyteczności publicznej

# OCEAN możliwości

WDROŻYLIŚMY OCEAN W URZĘDZIE MIASTA CIECHANÓW



Zadanie: Dostawa sprzętu komputerowego i oprogramowania oraz świadczenie usług w ramach projektu „Budowa i wdrożenie publicznego, interaktywnego systemu usług administracji samorządowej e-Urząd” (Etap I).

**ZAWSZE** się zastanawiam, dlaczego nazwy przetargów w administracji są takie smutne i skomplikowane, przecież systemy EOD, BOI i urzędy cyfrowe to systemy przynoszące korzyści wszystkim uczestnikom procesów administracyjnych.

OCEAN jako zwycięzca w przetargu najlepiej dopasował się do potrzeb zamawiającego.

Szczegółowym zadaniem postawionym OCEAN było wprowadzenie nowej jakości w obsłudze inte-

resanta w urzędzie miejskim. To właśnie „silnik” OCEAN Workflow, który napędza obieg dokumentów, rozsyłając je po poszczególnych stanowiskach w strukturze organizacyjnej i wybiegając daleko poza Biuro Obsługi Interesanta, sprawia, że nie interesant, a sprawa reprezentująca złożony dokument „biega” po piętrach urzędu.

O wyzwaniu rzuconym przez Prezydenta Miasta Ciechanowa opowiada Zastępca Kierownika projektu Michał Grabowski.

**Jakie wyzwania postawił Prezydent Ciechanowa podczas wdrażania Systemu Elektronicznego Obiegu Dokumentów OCEAN Workflow?**

**Michał Grabowski:** Pierwszym wyzwaniem była konieczność uświadomienia urzędnikom korzyści wynikających z pracy w Systemie Elektronicznego Obiegu Dokumentów. Dotychczas wydziały pracowały na odrębnych, specjalizowanych aplikacjach, a wymiana dokumentów odbywała się poprzez sekretariaty. Sprawiało to, że urząd generował wiele

dokumentów na wewnętrzne potrzeby. Problemy wynikające z braku współpracy między systemami i wielokrotność identyfikatorów dotyczących jednej sprawy sprawiły, że poszukiwanie informacji nie było łatwym zadaniem.

Drugim wyzwaniem było przewyciężenie przywiązania do dokumentów w wersji papierowej. Część urzędników była mało przygotowana do pracy z systemem informatycznym, spora ich grupa woli swój papier niż "pudełko" (dosłowny cytat), w które muszą pracownicy wstukiwać informacje (co zajmuje im jednak wciąż dużo czasu).

#### **Jak więc przekonałeś ich do podjęcia tej pracy?**

**MG:** Konieczne było przekonanie Zarządu Miasta, że raz wprowadzone do systemu dokumenty zawsze są dostępne, co nie jest cechą dokumentów papierowych.

Wyszukiwanie dokumentów powiązanych ze sprawą lub spraw podobnych w czasie mierzonym w sekundach przekonało ich do wzmożonego wysiłku i zainwestowania w pracę potrzebną na rejestrowanie dokumentów.

#### **Wspominałeś, że były problemy ze sprzętem...**

**MG:** Raczej z jego brakiem. Dostawa tak dużej ilości sprzętu w niesamowicie krótkim terminie była wyzwaniem samym w sobie. Sprzęt określony przez zamawiającego w SIWZ okazał się trudno dostępnym kąskiem dla koneserów. W związku z tym jego produkcja była ograniczona i dostawcy opóźnili terminy dostaw.

#### **Wiem, że pokonałście wszelkie trudności, ponieważ wdrożenie zostało zakończone.**

**MG:** Tak, system pracuje. Pikanterii wdrożeniu dodawał fakt współfinansowania przedsięwzięcia ze środków UE, przez co terminy oraz protokoły podlegały ścisłej kontroli formalnej. Dziś wiem, że prace dofinansowane, mimo iż szczegółowo zaplanowane i przemyślane na etapie studium wykonalności, są przez konieczne procedury przetargowe rozciągnięte w czasie. Od momentu napisania wniosku, poprzez ogłoszenie przetargu, do wykonania zadania i jego rozliczenia upływa sporo czasu. W tym samym momencie praca urzędu i dostępne technologie się zmieniają, często wykonując wielki skok organizacyjny bądź technologiczny.

#### **Proszę, opowiedz po kolei, jaka była Wasza droga do sukcesu.**

**MG:** W pierwszym tygodniu napotkaliśmy niespodziewany problem natury formalnej. Problem dotyczył łączenia sieci zewnętrznej z wewnętrzną. Instrukcja kancelaryjna wymagała odseparowania fizycznego obu sieci, co w rzeczywistości jest praktycznie nie do zrealizowania. Chodziło oczywiście o odseparowanie logiczne obu sieci. Sprawa stanęła niemal na ostrzu noża. Problem udało się rozwiązać dzięki interwencji pracowników ciecha-

nowskiego UM w Ministerstwie Spraw Wewnętrznych i Administracji.

Dodatkowym dużym utrudnieniem wdrożenia było nieumyślne pominięcie na etapie analizy przez przedstawicieli zamawiającego wiedzy o szczegółach procesów zachodzących w urzędzie. Dla urzędników wiele procesów zachodzących w administracji było oczywistych i nieistotnych dla całego przedsięwzięcia. System informatyczny jednak musi w swojej funkcjonalności uwzględniać wszystkie przypadki. Dobrym przykładem ilustrującym ten problem są wyjątki od standardowych procedur, które w sposób wielokrotny zwiększyły definicje nawet najprostszyc procesów.

Na szczęście zespołem wdrożeniowym po obu stronach zależało na skutecznym wdrożeniu, więc problemy rozwiązywano sukcesywnie.

#### **Co system dał interesantom?**

**MG:** Podstawową korzyścią dla interesantów jest możliwość wysyłania wniosków przez Internet i otrzymywania odpowiedzi o stanie sprawy. Takiej funkcjonalności interesanci wcześniej nie mieli. Najprawdopodobniej w pierwszej kolejności z tej funkcjonalności skorzystają przedsiębiorcy i osoby młodsze, posiadające doświadczenie i dostęp do Internetu. Dla osób preferujących tradycyjną formę komunikacji pracuje Biuro Obsługi Interesanta, którego zadaniem jest kompleksowa obsługa poszczególnych spraw zgłaszanych przez interesantów.

Praktycznie całkowicie uległa zmianie procedura kontaktu urzędu z interesantem. Wcześniej to interesant chodził od biurka do biurka, często nie uzyskując kompleksowej informacji o elementach sprawy. Dziś spotkanie odbywa się w jednym, komfortowym miejscu, gdzie interesant przyjmowany jest przez kompetentnego urzędnika procesującego sprawę w imieniu interesanta w wydziałach urzędu.

#### **Co system dał urzędnikom?**

**MG:** OCEAN Workflow zapewnia skuteczny nadzór nad dokumentami oraz sprawami toczącymi się w urzędzie. Sprawy są w jasny, jednoznaczny i określony przez obieg dokumentów sposób procesowane od stanowiska do stanowiska. System w pełni kontroluje terminowość realizacji poszczególnych zadań składających się na sprawy.

Stan sprawy zgłoszonej poprzez elektroniczną skrzynkę podawczą publikowany jest w części Biuletynu Informacji Publicznej nazwanej Cyfrowym Urzędem. Dotarcie do szczegółów sprawy zajmuje minimalną ilość czasu, uwzględniając przy tym sprawy z okresów wcześniejszych.

#### **Czy Zarząd Miasta może skontrolować pracę urzędu?**

**MG:** Tak, elementem systemu jest moduł Informowania Kierownictwa, dzięki któremu możliwa

jest kontrola stanu spraw w urzędzie przez przełożonych.

W szczególności dostępne są raporty ilościowe i jakościowe spraw toczących się w urzędzie. System taki umożliwia wyznaczanie zastępstw w przypadku absencji chorobowej urzędników, powodując równomierne rozłożenia zadań i zakończenie spraw w toku.

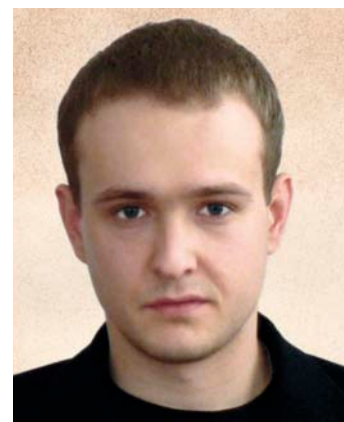
#### **Czy po zainstalowaniu systemu praca urzędników się poprawiła?**

**MG:** Docelowo tak, wszystkie procedury uległy przyspieszeniu, urzędnicy mają łatwiejszy dostęp do informacji. "Docelowo", ponieważ w okresie przejściowym to jest nawet przeciwnie – jest wolniej i trudniej, gdyż obieg elektroniczny obecnie nie zastąpił jeszcze obiegu papierowego. Decyzję o rezygnacji z obiegu dokumentów drogą papierową podejmie Zarząd miasta.

#### **Słyszałem, że w czasie wdrożenia w UM Ciechanów OCEAN Workflow został wybrany w innych jednostkach.**

**MG:** Tak, to prawda. Co najmniej 3 klientów zdecydowało się na wdrażanie OCEAN w swoich instytucjach w przeciągu ostatnich kilku miesięcy, ale o tym możemy porozmawiać po zakończeniu wdrożeń...

*Rozmowę przeprowadził Łukasz Tylkowski*



**Michał Grabowski**

#### **Comarch SA**

**Stanowisko:** Kierownik Centrum Produkcyjno-Wdrożeniowego

**Sektor:** Administracja Publiczna, Utilities i Samorządy (APUS)

**Info:** W Comarch zajmuje się OCEAN Workflow



# Rozwiązania na miarę nagród

Przyznawane regularnie nagrody i wyróżnienia na bieżąco wyznaczają nowe trendy w branży IT oraz stanowią potwierdzenie sprawdzonych i efektywnych systemów.

„GAZETA Bankowa”, „Miesięcznik Finansowy BANK” czy specjalistyczne jury na konferencjach branżowych pełnią funkcję recenzenta i dostarczają rzetelnych informacji o sytuacji na rynku finansowym i bankowym, gdzie poprzeczka podnoszona jest coraz wyżej. Coraz większe wymagania sektora oraz prężnie rosnąca konkurencja wymuszają na firmach IT nowatorskie rozwiązania oraz elastyczne i bezpieczne systemy. Comarch wydaje się radzić sobie bardzo dobrze w tym środowisku, czego potwierdzeniem są kolejne wyróżnienia i nagrody. W ostatnim czasie Comarch zajął III miejsce w rankingu IT@BANK na „Najlepsze firmy informatyczne dla sektora finansowego 2008”, otrzymał wyróżnienie w konkursie „Hit roku dla instytucji finansowych” za system Pl@net wersja3 wdrożony w Fortis Bank Polska oraz nagrodę Złoty Bit GigaCon 2008 za najlepszy system CRM.

### Platforma CAFÉ oraz Comarch Internet Banking

Comarch ukłasyfikował się w pierwszej trójce „Najlepszych firm informatycznych dla sektora finansowego 2008” w rankingu IT@BANK, przeprowadzonym od trzech lat przez „Miesięcznik Finansowy BANK”. W tegorocznej edycji niezależni bankowi analitycy finansowi dokonali porównania i oceny 38 najlepiej prosperujących firm informatycznych świadczących usługi dla banków i sektora finansowego. Szczegółowej analizie dokonano w oparciu o kryterium wysokości przychodów, udziału przychodów od sektora finansowego oraz sektora publicznego, liczby produktów z danej kategorii, liczby zatrudnionych oraz rentowności działania.

Na to prestiżowe wyróżnienie dla Comarch w obszarze finansów i bankowości złożyła się cała gama sukcesów. Warto w tym miejscu wspomnieć o Platformie CAFÉ Comarch Front-End, będącej kompletnym środowiskiem pracy dla oddziałów, Contact Center oraz innych placówek instytucji finansowych, która została już nagrodzona rekomendacją „Gazety Bankowej”. Również systemy bankowości internetowej Comarch Internet Banking zyskują coraz większą popularność, szczególnie po głośnych wdrożeniach w Fortis Bank, Banku BPH, PEKAO SA czy NORD/LB Bank Polska.

### Platforma CAFÉ

Platforma CAFÉ integruje wiele systemów biznesowych oraz dostarcza intuicyjnego i ergonomicznego interfejsu pracy, stanowiąc jednolitą platformę technologiczną, w której osadzone są wszystkie moduły funkcjonalne dostępne dla użytkowników. Dzięki zastosowaniu architektury por-

tletów, jak również oparciu platformy na systemie Comarch CMS możliwe jest pełne biznesowe zarządzanie formą i zawartością systemu widzanego oczami użytkownika. Dużo łatwiejsze staje się dostosowywanie środowiska pracy do zmieniających potrzeb biznesowych, jak również łączenie funkcjonalności biznesowych z informacyjnymi czy nawet intranetem. Pracownik loguje się tylko do jednego systemu, w którym ma wszystkie potrzebne opcje, poczynając od informacji ogólnofirmowych, a kończąc na operacjach gotówkowych wykonywanych w kasie. Rozwiązanie to oferuje cały szereg korzyści:

- ▶ **Efekt synergii.** Dzięki zgromadzeniu w jednej wspólnej platformie wysokiej jakości systemów doskonale przygotowanych do realizacji postawionych przed nimi wymagań użytkownik otrzymuje dodatkowy efekt synergii i zwielokrotnia efekty wdrożenia.
- ▶ **Usprawnienie i ujednoczenie interfejsów systemów informatycznych.** Ergonomiczne i przyjazne środowisko podnosi jakość i efektywność zadań wykonywanych przez pracowników. W rezultacie prowadzi to do redukcji kosztów związanych ze szkoleniami czy bezproduktywnym czasem potrzebnym na przelogowywanie lub przenoszenie danych z aplikacji do aplikacji.
- ▶ **Modułarna architektura.** Ta cecha pozwala na ewolucyjne budowanie rozwiązania „z klocków”. Najpierw tworzy się jądro systemu, a następnie w prosty sposób rozbudowuje się system, dołączając kolejne moduły.
- ▶ **Możliwości konfiguracyjne.** Elastyczność w zarządzaniu pozwala szybko reagować na zmiany w uwarunkowaniach biznesowych i modyfikacje platformy, bez konieczności angażowania osób technicznych zarówno w zakresie struktury systemu, jak i procesów biznesowych.
- ▶ **Uspójnienie mechanizmów bezpieczeństwa i administracji.** Skutkiem zastosowania jednolitych rozwiązań jest możliwość centralnego zarządzania użytkownikami i wprowadzenia spójnej polityki bezpieczeństwa.

### Comarch Internet Banking

Kolejnymi produktami, które miały duży wpływ na zdobycie przez Comarch tak wysokiego miejsca w rankingu IT@BANK, są systemy Comarch Internet Banking:

- ▶ Comarch Retail Internet Banking
- ▶ Comarch Corporate Internet Banking

Internetowe rozwiązania oferowane bankom detalicznym wyróżniają się precyzyjnie opracowaną technologią cienkiego klienta, która jest znacznie tańsza w utrzymaniu i rozwoju od standar-

dowych systemów opartych o grubego klienta. System zapewnia klientom detalicznym oraz mikroprzedsiębiorstwom dostęp do usług oferowanych przez bank 7 dni w tygodniu, 24 godziny na dobę, za pomocą Internetu, WAP, SMS oraz innych kanałów dystrybucyjnych. Rozwiązanie to stanowi uniwersalne, kompletne, wydajne i bezpieczne uzupełnienie środowiska informatycznego banku o bogatej i łatwej w rozszerzeniu funkcjonalności. Natomiast nowoczesne relacje z klientem korporacyjnym pomaga kształtować Comarch Corporate Internet Banking. System jest zoptymalizowany pod kątem masowego przetwarzania płatności, podziału ról w przedsiębiorstwie, wsparcia dla komunikacji między klientem a opiekunem ze strony banku oraz najwyższego dostępnego poziomu bezpieczeństwa.

W 2005 r. Comarch Internet Banking wdrożony w Banku BPH, najlepszym europejskim banku internetowym dla klientów korporacyjnych w 2005 r., został wyróżniony nagrodą w konkursie „The European Banking technology” w kategorii „The Best Customer Relationship Achievement”. Rok później Bank BPH uznano za najlepszy Bank Finansowania Handlu w Polsce w 2006 r. na łamach międzynarodowego magazynu „Global Finance”.

### Comarch Pl@net

Kolejnym systemem, na który w ostatnim czasie „Gazeta Bankowa” zwróciła uwagę swoich czytelników i nie tylko, był zrealizowany przez Fortis Bank i Comarch system bankowości internetowej Comarch Internet Banking Pl@net. Projekt został wyróżniony w konkursie „Hit roku dla instytucji finansowych” w kategorii „Bankowość elektroniczna i e-finance” w ramach VI edycji konkursu na najlepszy projekt informatyczny wdrożony w 2007 roku w instytucjach finansowych. Rozwiązanie łączy w sobie prawie wszystkie produkty oferowane przez bank w ramach portfolio produktowego. Platforma składa się z systemu Pl@net skierowanego do klientów indywidualnych w zakresie produktów bankowych i funduszy inwestycyjnych oraz BiznesPl@net przeznaczonego dla firm. Rozwiązanie redukuje potrzebę bezpośredniego kontaktu klienta z bankiem do minimum. Użytkownicy komunikują się z systemem za pomocą standardowej przeglądarki internetowej. Internet Banking Pl@net charakteryzuje się przede wszystkim:

- ▶ **Wysokim bezpieczeństwem.** Wzmocniono systemy, wyeliminowano zagrożenia typu SQL Injection, Scoss-Site Scripting i tym podobne, przeprowadzając je przez zewnętrzną firmę. Bezpieczeństwo zapewnia też komunikacja wymuszająca korzystanie ze 128-bitowego protokołu

SSL 3.0, mechanizmy zapobiegające phishingowi oraz eliminujące key-loggery, takie jak spersonalizowane klawiatury oraz mechanizmy powiadamiające o zdarzeniach w systemie. Wbudowany jest także autonomiczny system zarządzania dostępem oraz mechanizmy kontroli sesji (pojedyncza sesja, wygasanie sesji i brak możliwości używania cofania się do poprzedniego ekranu przez ikonę „wstecz” w przeglądarce internetowej).

▶ **Funkcjonalnością.** Pl@net umożliwia efektywne zarządzanie wszystkimi produktami bankowymi: rachunkami, kartami, kredytami i produktami inwestycyjno-oszczędnościowymi.

▶ **Kompleksową strukturą.** Pl@net zapewnia zintegrowany dostęp do wszystkich rachunków i produktów bankowych. Ponadto daje możliwość przejścia w prosty sposób z ekranów obsługujących prywatne finanse do rachunków firmy, bez konieczności powtórzonego przelogowywania.

▶ **Łatwością w użyciu i niezawodnością.** Cechą charakterystyczną systemu jest duża przejrzystość prezentacji danych i intuicyjność użytkownika, dzięki czemu korzystanie z niego nie stwarza problemów nawet tym osobom, które wcześniej nie korzystały z bankowości internetowej. System stanowi gwarancję dostępu do zawsze aktualnych danych i usług bankowych.

Oprócz systemu Pl@net w Fortis Bank Polska na polskim rynku spośród platform Comarch Internet Banking wdrożono również:



**Maria Sulisz**

Comarch SA

**Stanowisko:** Specjalista ds. Marketingu

**Sektor:** Finanse, Bankowość i Ubezpieczenia

▶ Raiffeisen on-line w Raiffeisen Bank Polska w 2007 r.

▶ ING BankOnLine w ING Banku Śląskim w 2007 r.

▶ PekaoBIZNES24 w Banku PEKAO / Unicredit Group w 2005 r.

▶ Sez@m w Banku BPH / Unicredit Group w 2004 r.

▶ BusinessNet w Banku BPH / Unicredit Group w 2004 r.

▶ Nordnet w DnB Nord Polska w 2004 r.

Obecnie przed produktem stoją wyzwania dostosowania do wymogów rynków zagranicznych pod względem formatów, przepisów prawnych oraz integracji z systemami lokalnymi, jak również standardów Komisji Europejskiej (SEPA).

## Comarch Analytical CRM

Nowe rozwiązanie Comarch Analytical CRM (aCRM) zdobyło ostatnio publiczną akredytację w postaci nagrody Złoty Bit 2008 w dziedzinie doskonalenia narzędzi wspierających utrzymywanie efektywnych relacji z klientami. Wyróżnienie stanowi wyraz uznania członków kadry zarządzającej zgromadzonych na IV Konferencji CRM GigaCon w Warszawie. Comarch aCRM jest nowatorskim na polskim rynku systemem analityczno-decyzyjnym. Program ma spełniać rolę inteligentnego doradcy o strukturze arkusza kalkulacyjnego, rozbudowanego o szeroką paletę narzędzi statystycznych oraz szereg nowoczesnych metod obliczeniowych, jak np. algorytmy Data Mining służące do segmentacji oraz klasyfikacji klientów. Program podpowiada konsultantowi obsługującemu klienta, czym klient byłby najprawdopodobniej zainteresowany oraz jakie będą prawdopodobnie jego przyszłe decyzje wobec usługodawcy. Działanie algorytmów Data Mining oparte jest na poszukiwaniu w bazie danych wzorców przyczynowo-skutkowych, a następnie „wylczeniu” nieznanego skutku, gdy znana jest przyczyna.

*Elementarnym przykładem działania systemu jest bank, który chce wypromować nowy kredyt mieszkaniowy. Nie chcąc przygotowywać oferty masowej, bank staje przed problemem wyboru grupy docelowej. Po uruchomieniu aCRM, podłączeniu bazy danych klientów oraz wskazaniu systemowi kolumn z odpowiednimi informacjami rozpoczyna się analiza mająca na celu wykrycie przyczyn (tj. cech klienta), które decydują o skutku w postaci zaciągniętego kredytu. Następnie system zwraca reguły, które będą klasyfikować dowolnego klienta jako potencjalnie chętnego na wzięcie kredytu. Przykładowy zestaw reguł: jeśli klient nie ma mieszkania na własność oraz jeśli jego wiek jest w przedziale 25-35, oraz zarabia więcej niż 4000 brutto, oraz... itd., to prawdopodobnie jest zainteresowany wzięciem*

*kredytu. Odkryte reguły implementowane są następnie w systemie, a ich wynik wyświetlany na ekranie monitora konsultanta obsługującego klienta. Konsultant wie wobec tego, czy jest sens proponować obsługiwane klientowi kredyty, czy nie. Oczywiście to jest bardzo błahy przykład; aCRMy są wykorzystywane do znacznie bardziej złożonych i mniej intuicyjnych analiz – tłumaczy Bartłomiej Kozakowski, Business Solutions Manager, Comarch SA.*

*Wszystko zależy od profilu firmy, która używa tego systemu. Ogólnie wszystko sprowadza się do tzw. personalizacji obsługi klienta. Klient, nawet anonimowy, powinien w wielkiej instytucji, która obsługuje tysiące jemu podobnych, czuć się tak, jakby robił zakupy na przydomowym bazarze, gdzie każdy sprzedawca od lat zna jego upodobania i potrzeby. Klient powinien mieć poczucie, że będzie obsłużony zgodnie z jego realnymi potrzebami, a nie tymi, które wymuszane są przez masowe akcje marketingowe. Jest to pierwsze, ogólne przeznaczenie systemu. Bardziej szczegółowymi przykładami zastosowania mogą być: dla banku fakt, czy klient spłaci kredyt oraz czy w przyszłości wartość klienta wzrośnie, dla firmy ubezpieczeniowej poziom ryzyka związany z konkretnym profilem klienta. Dla sieci stacji paliw – poziom lojalności klienta. Dla producenta ekskluzywnych towarów – najlepsza grupa docelowa klientów. Dla detaliści ciekawa może być tzw. analiza koszykowa, czyli tworzenie pakietów promocyjnych itd. Zastosowań mogą być tysiące – kontynuuje Bartłomiej Kozakowski.*

aCRM jest „silnikiem analitycznym” systemu Comarch CRM. Może on funkcjonować niezależnie jako zwykły pakiet obliczeniowy, jednak jego prawdziwa, unikalna wartość pojawia się, gdy działa w roli doradcy konsultanta, tj. gdy modele analityczne przekształca się w realne działania biznesowe. Program stanowi wciąż nowatorskie na polskim rynku rozwiązanie.

*W Polsce mało kto słyszał o tego typu systemach, w USA jednak już od ponad 10 lat przynoszą one ogromne zyski instytucjom, które je wdrożyły, a rynek pracy pęka od ogłoszeń poszukujących ludzi znających techniki modelowania danych. Nawet więc jeśli ciągle nie ma dostatecznego zaufania do systemów, które podpowiadają, co robić, to potrzeba ich rychłego wdrożenia jest coraz większa, tak samo jak liczba klientów, którzy sobie to uświadamiają. Swoją drogą, w ten właśnie sposób tłumacząc fakt przyznania nam nagrody na Konferencji GigaCon – komentuje Bartłomiej Kozakowski.*



# ITIL -

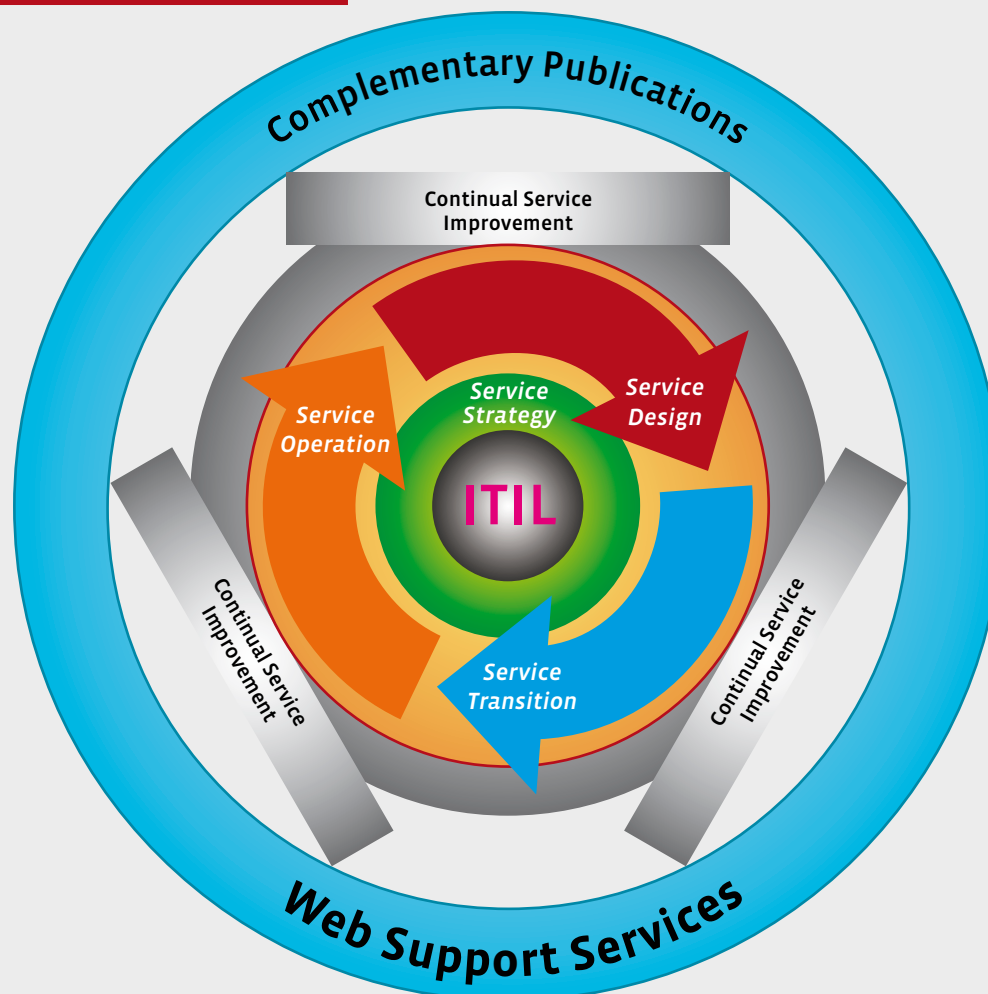
# koszt czy wartość dodana?

Do niedawna outsourcing systemów informatycznych odbywał się na zasadzie negocjacji kontraktu pomiędzy stronami. Nie występowały żadne zalecenia dotyczące sposobu obsługi podmiotu outsourcowanego. Stan taki powodował wiele konfliktów i nieporozumień na osi przedsiębiorstwo – firma outsourcingowa.

**RZĄD** brytyjski niezadowolony z jakości usług świadczonych przez firmy informatyczne zlecił opracowanie standardów zarządzania w sferze informatycznej. W ten sposób powstał ITIL.

ITIL (Information Technology Infrastructure Library) jest zbiorem reguł opartych na najlepszych praktykach w dziedzinie zarządzania IT; został wypracowany przez: ekspertów, konsultantów, dostawców rozwiązań IT oraz końcowych użyt-

kowników IT. Metodyka ITIL zawiera zestaw powiązanych ze sobą najlepszych praktyk dla obniżenia kosztów IT, przy jednoczesnym podnoszeniu jakości usług IT świadczonych użytkownikowi. ITIL jest obecnie uważany za najpełniejsze podejście do

**Rysunek 1. Struktura biblioteki ITIL**

Źródło: itSMF, Foundations of IT Service Management, based on ITIL

zarządzania usługami IT i stanowi de facto światowy standard w tej dziedzinie<sup>1</sup>.

ITIL opisuje i definiuje kluczowe procesy oraz sposób zarządzania usługami IT, takimi jak: obsługa problemów, zmiany konfiguracji i instalowanie nowych wersji czy zarządzanie zmianami. Dzięki takiemu podejściu działy IT zostają wyposażone w narzędzia do identyfikacji procesów wewnątrz IT. Nieważne, czy organizacja jest mała, duża czy średnia, ITIL pozwala na stworzenie podstaw do analizy procesów, jakim podlega informatyka w odniesieniu do całego przedsiębiorstwa<sup>2</sup>.

Pierwsza wersja metodyki ITIL została opublikowana w 1989 r. Na bibliotekę ITIL w najnowszej wersji – trzeciej, ogłoszonej w maju 2007 r., składa się 5 następujących publikacji (tomów):

- » Service Strategy (SS) – Strategia w zarządzaniu usługami informatycznymi
- » Service Design (SD) – Projektowanie usług

- » Service Transition (ST) – Wdrażanie usług
- » Service Operation (SO) – Utrzymanie usług
- » Continual Service Improvement (SCI) – Mechanizmy ciągłego doskonalenia usług.

### Korzyści

ITIL prezentuje podejście procesowe do zarządzania usługami IT. Definiuje cele, główne czynności oraz sposób rozpoczynania i kończenia procesu. Daje szereg wskazówek dotyczących pomiarów, raportowania oraz audytu procesów w celu weryfikacji i podnoszenia jakości świadczonych usług. Model ten jest w pełni skalowalny, tzn. odpowiedni dla przedsiębiorstw o różnej wielkości, jak i profilu działania.

Wdrożenie metodyki ITIL w przedsiębiorstwie pozwala m.in. na:

- » obniżenie kosztów obsługi procesów informatycznych,

- » poprawę dostępności, niezawodności i bezpieczeństwa świadczonych usług IT,
- » wzrost wydajności realizowanych projektów IT,
- » lepsze wykorzystanie zasobów informatycznych, w tym także dostawców zewnętrznych,
- » dostarczenie usług zgodnych z potrzebami klienta biznesowego i użytkownika końcowego.

ITIL daje również wiele korzyści niezwiązanych bezpośrednio z wprowadzeniem konkretnych procesów, a przede wszystkim definiuje wspólny język pomiędzy dostawcami usług IT a biznesem (sponsorem). Organizacja stosująca ITIL jest postrzegana jako profesjonalista na rynku i powoli niemożliwe staje się świadczenie usług informatycznych bez wdrożenia „dobrych zasad” ITIL.

## ITIL a Comarch

Obecnie wiele firm produkcyjnych i usługowych ponosi duże nakłady inwestycyjne w bardzo skomplikowaną infrastrukturę informatyczną. Firmy te najczęściej nie optymalizują swoich procesów zarządzania usługami IT, gdyż usługi informatyczne nie są ich podstawową działalnością i szeroko rozumiana informatyka traktowana jest, kolokwialnie mówiąc, jako „zło konieczne”. Pomocne jest tutaj wdrożenie najlepszych praktyk oferowanych przez bibliotekę ITIL, które poprzez optymalizację procesów zarządzania IT pomagają uzyskać większe korzyści z inwestycji w infrastrukturę.

I. Wells, D. Lonsdale i A. Jeffcoat w artykule *Ten Tips for Successfully Implementing ITIL* omawiają kluczowe zagadnienia umożliwiające wdrożenie biblioteki ITIL z sukcesem. Są to m.in.:

- » określenie realistycznych celów oraz punktu, w odniesieniu do którego można prowadzić ulepszenia,
- » zaangażowanie do wdrożenia jak największej grupy pracowników na różnych szczeblach organizacji; kluczowa jest również komunikacja przy procesie implementacji,
- » traktowanie wdrożenia modelu ITIL jako części ogólnej strategii obejmującej całe IT w przedsiębiorstwie,
- » uwzględnienie w projekcie procesów IT wizji całej organizacji po zakończonej już implementacji,
- » zrozumienie wpływu procesów na siebie nawzajem, które pozwoli osiągnąć maksymalne korzyści z wdrożenia biblioteki ITIL.

Koszt wdrożenia ITIL w organizacji to duże nakłady na zbudowanie odpowiednich procedur i zdefiniowanie procesów dopasowanych do danego przedsiębiorstwa. Wdrożenie ITIL to także duże zaangażowanie osób odpowiedzialnych za implementację modelowych procesów. Bez aktywnego poparcia i uczestnictwa kierownictwa najwyższego szczebla wdrożenie ITIL w przedsiębiorstwie staje się praktycznie niemożliwe.

Koszt wdrożenia ITIL można znacznie obniżyć przez „wykupienie know-how”, czyli zaangażowanie firmy świadczącej usługi typu „IT Management”.

Comarch w trakcie realizacji projektów outsourcingowych świadczy usługi zarządzania środowiskiem IT. Gwarantuje przy tym optymalne działanie całej infrastruktury IT jako jednego spójnego środowiska, zapewnia modelowanie procesów informatycznych oraz ich optymalizowanie. Zapewnia także dostosowanie infrastruktury do zmian w przedsiębiorstwie, prawie, technologii. Usługa świadczona jest przez wyspecjalizowaną kadrę, profesjonalne narzędzia oraz wykorzystuje m.in.



metodykę ITIL. Comarch od kilku lat świadczy usługi outsourcingu IT. Jako referencje mogą posłużyć wdrożenia w GK Kęty, Elektrowni Skawina, Santander Consumer Banku, Renault i wiele innych.

## Wnioski

Niewątpliwym wyzwaniem związanym z wdrożeniem ITIL jest zmiana sposobu myślenia o informatyce i usługach IT. „Informatyka” jest dla biznesu i musi rozmawiać z biznesem zrozumiałym językiem, sprawiając, żeby biznes był wciąż bardziej konkurencyjny, bardziej efektywny i ograniczał koszty.

Na podstawie doświadczeń i licznych case studies można wysnuć wniosek, że ITIL to nie koszt poniesiony przez przedsiębiorstwo, to nie wartość dodana do kontraktu outsourcingowego, ale to konieczność. Każda firma, której działalność wspierana jest usługami świadczonymi przez działy informatyczne, musi poważnie zastanowić się nad wdrożeniem procedur, które usprawnią działanie usług informatycznych i dadzą pewność ciągłości działania. Dopiero wówczas będzie można w pełni skupić się na działalności podstawowej przedsiębiorstwa – osiągnięciu zysku.

### Przypisy

- 1 Forrester Research, ITIL's Final Breakthrough: From 'What' to 'How', 2004
- 2 it Service Management Forum

Warto również przeczytać:

<http://www.best-management-practice.com>

<http://www.itlife.pl/>

<http://www.itsmf.org/>



## Andrzej Nowacki

Comarch SA

**Stanowisko:** Konsultant ds. Outsourcingu Infrastruktury

**Sektor:** Usługi

**Info:** Od 9 lat pracuje w Comarch jako kierownik projektów, zrealizował wdrożenia m.in. dla: PEKAO SA, BP Polska, MEN, Elektrowni Skawina, Santander Consumer Bank



# Wirtualizacja

CZAS NA PRZYSZŁOŚĆ

Hasło „wirtualizacja zasobów IT” zdobywa i podbija dzisiaj cały świat. Szaleństwo wirtualizacji jakiś czas temu trafiło również do Polski i zagościło już na dobre w rodzimych serwerowniach.

**DZIS** wirtualizować można prawie wszystko – serwery, pamięci masowe, sieci, systemy operacyjne i aplikacje biznesowe. W tej chwili w centrach danych największe korzyści daje wirtualizacja serwerów – pozwala nie tylko na znaczne oszczędności, ale także upraszcza zarządzanie fizyczną infrastrukturą, coraz bardziej rozbudowaną w środowiskach IT.

## Co nieco o historii wirtualizacji, czyli tytułem wstępu

Historia wirtualizacji wbrew pozorom wcale nie jest taka krótka i nie jest na pewno kwestią chwilowej mody, dominującej akurat w dzisiejszych czasach. Pierwsze mechanizmy wirtualizacyjne pojawiły się już w latach 50. ubiegłego stulecia, aczkolwiek były one w pewnym sensie efektem ubocznym opracowanej technologii. Dopiero dekadę później zaczęto wykorzystywać opracowane mechanizmy do realizacji zadań, które dzisiaj kojarzą nam się jednoznacznie z wirtualizacją – rozpoczęło się tworzenie i użytkowanie wirtualnych środowisk w oparciu o fizyczne zasoby obliczeniowe; środowisk tych jednak nie można było ani dotknąć, ani namacalnie sprawdzić. Prawdziwa nowość! Dzisiaj wielu z nas wydaje się to niepojęte, a co dopiero pół wieku temu...

Prawdziwa eksplozja popularności zaczęła się jednak dopiero parę lat temu. Firma VMware była co prawda wtedy już dość znana na rynku IT, jednak stworzona przez nią technologia uchodziła przez długi czas za niszową, trudno było znaleźć dla niej praktyczne zastosowania, chociaż wszy-

scy eksperci podkreślali jej zalety, innowacyjność i wysoki poziom zaawansowania technologicznego. No i w końcu zaczęło się.

Skoro w jednym fizycznym serwerze można upchnąć wiele osobnych maszyn, środowisk systemowych, to właściwie dlaczego tego nie robić? Przecież wiele z istniejących systemów pracuje nieefektywnie, zasoby ich są nieoptymalnie wykorzystane, wiele z nich to środowiska niekrytyczne z punktu widzenia biznesowego (wszelakie systemy do celów testowych, rozwojowych, szkoleniowych) lub nawet traktowane jako zwykłe generatory kosztów – środowiska zapasowe, które 99,99 proc. czasu po prostu się nudzą. Zastosowanie wirtualizacji to czysty zysk dla firmy – na pierwszy rzut oka: mniej sprzętu w serwerowniach, większe możliwości rozbudowy, inwestycji, mniejsze koszty utrzymania, mniejsze koszty zasilania i klimatyzacji centrum danych. Jednym słowem – realne pieniądze, które pozostają w kieszeni firmowej, i krok do praktycznej realizacji „Green DataCenter”. Żeby nie być gołosłownym – u jednego z polskich operatorów telekomunikacyjnych ponad 150 serwerów można było zastąpić ledwie dwudziestoma, a w dużym banku – na kilku serwerach uruchomionych zostało 250 partycji z różnego rodzaju usługami biznesowymi.

## Wirtualizacja VMware

VMware Infrastructure to pierwszy na rynku kompletny pakiet do wirtualizacji, umożliwiający przekształcenie i zoptymalizowanie infrastruktury systemów informatycznych oraz zarządzanie tą infrastrukturą poprzez wirtualizację. Umożliwia on

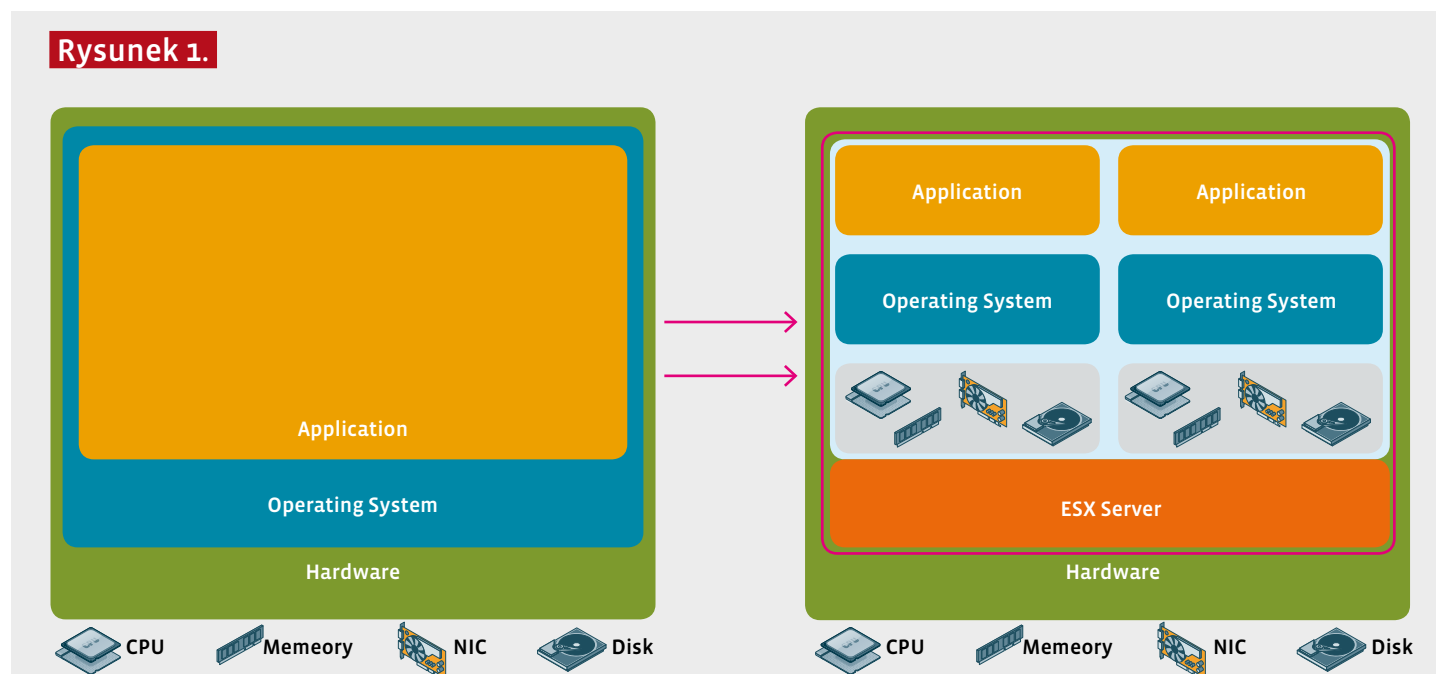
centralne zarządzanie wirtualnymi środowiskami, optymalizację zasobów, zwiększa dostępność aplikacji i automatyzuje działania operacyjne. Dzięki temu pozwala zarówno na oszczędności finansowe, jak też eliminację konieczności niepotrzebnego wykonywania powtarzających się czynności operacyjnych, zwiększając jednocześnie dostępność całej infrastruktury i podnosząc poziom świadczenia usług biznesowych.

Pakiet VMware Infrastructure pozwala stworzyć szybkie, dynamiczne i wydajne środowisko informatyczne o wysokiej dostępności. Infrastruktura wirtualna eliminuje wiele ograniczeń tradycyjnej infrastruktury sprzętowej, w której warstwa aplikacyjna jest przypisana do przydzielonego jej zasobu serwerowego.

## Korzyści płynące z budowy infrastruktury wirtualnej jest wiele:

- ▶ **Konsolidowanie serwerów.** Ograniczenie rozproszenia serwerów poprzez uruchamianie aplikacji w serwerach wirtualnych, na mniejszej liczbie wysoce skalowalnych fizycznych serwerów klasy Enterprise. Odnotowywany jest wskaźnik konsolidacji sięgający 1:10, czyli 10 maszyn wirtualnych przypadających na 1 rdzeń procesora.
- ▶ **Zapewnienie ochrony ciągłości biznesowej przy niższych kosztach.** Pakiet VMware Infrastructure gwarantuje wysoką dostępność aplikacji o znaczeniu krytycznym. Pozwala wdrożyć ujednoczoną platformę odtwarzania po awarii, która umożliwia przywrócenie wielu eksploatacyjnych

Rysunek 1.



maszyn wirtualnych w przypadku awarii sprzętu. Nie są konieczne inwestycje w kosztowne odwzorowywanie typu „1 do 1” sprzętu eksploatacyjnego i zapasowego.

▶ **Udoskonalenie testów i opracowywania oprogramowania.** Konsolidacja oddzielnych środowisk programistycznych, testowych i etapowych opartych na wielu systemach operacyjnych i wielowarstwowych aplikacjach.

▶ **Uproszczenie wdrażania infrastruktury.** Krótki czas wdrożenia kolejnych serwerów wirtualnych dzięki wbudowanej automatyce. Scentralizowany nadzór i odpowiedzialność za zasoby sprzętowe przy jednoczesnym przekazaniu oddziałom i właścicielom aplikacji pełnej kontroli nad wykorzystaniem zasobów.

▶ **Ponowne udostępnienie starszych aplikacji.** Migracja starszych systemów operacyjnych i aplikacji do maszyn wirtualnych uruchomionych na nowym sprzęcie w celu zwiększenia ich niezawodności.

## Korzyści z zastosowania wirtualizacji VMware

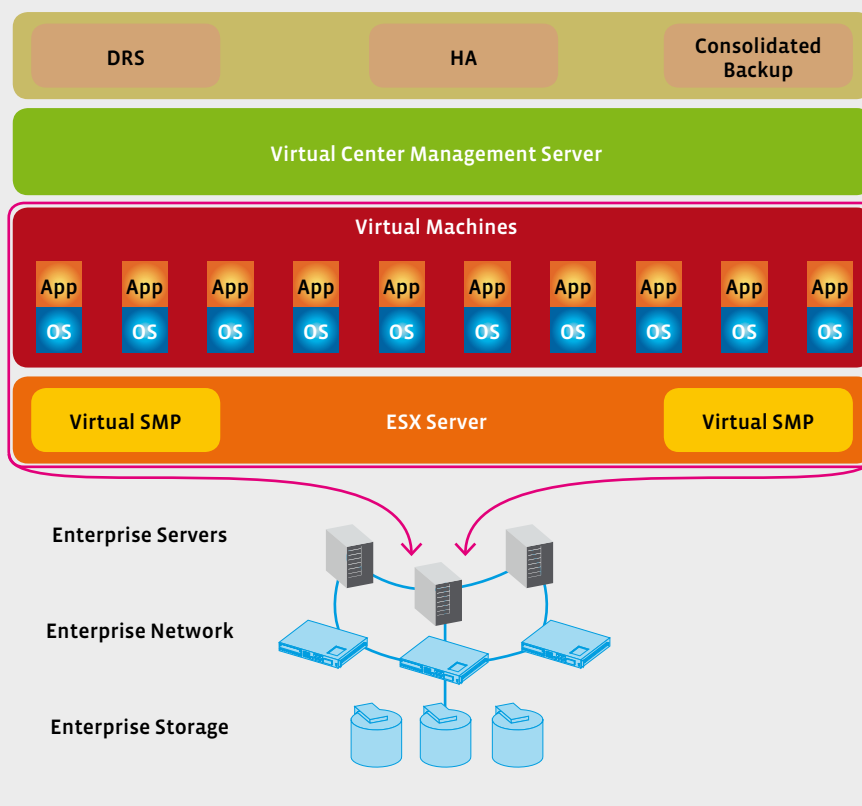
Oprogramowanie VMware Infrastructure daje wymierne oszczędności w kosztach operacyjnych.

- ▶ Zwiększa poziom wykorzystania sprzętu i ogranicza wymagania sprzętowe.
- ▶ Ogranicza koszty utrzymania przestrzeni serwerowej i energii elektrycznej.
- ▶ Obniża koszty pracy przez uproszczenie i automatyzację czynności i zasobochłonnych operacji informatycznych w rozproszonych środowiskach sprzętu, systemów operacyjnych i aplikacji.
- ▶ Zapewnia dostępność aplikacji oraz ciągłość biznesową niezależnie od sprzętu i systemów operacyjnych.
- ▶ Umożliwia nieprzerwaną pracę i konserwację bez przestoju w środowiskach informatycznych.
- ▶ Eliminuje konieczność czasochłonnej instalacji i konfiguracji oprogramowania dzięki pre-konfigurowanym template'om serwerów wirtualnych.
- ▶ Przyspiesza cykle opracowywania i wdrażania aplikacji.
- ▶ Skraca czas reakcji na potrzeby biznesowe dzięki dynamicznej optymalizacji środowisk aplikacji.
- ▶ Umożliwia współpracę starszych systemów i nowych rozwiązań sprzętowych.

## Jak działa VMware Infrastructure?

Pakiet VMware Infrastructure oddziela system operacyjny od sprzętu, na którym jest uruchomiony. Zapewnia warstwę wirtualną, która emuluje procesor, pamięć, dyski i zasoby sieciowe, udostępnia-

## Rysunek 2. Jak działa VMware Infrastructure?



jąc je wielu maszynom wirtualnym. Posługując się techniką wirtualizacji, można łatwo konsolidować obciążenie wielu całkowicie odmiennych serwerów na bardziej niezawodnym sprzęcie, pracującym z większą wydajnością.

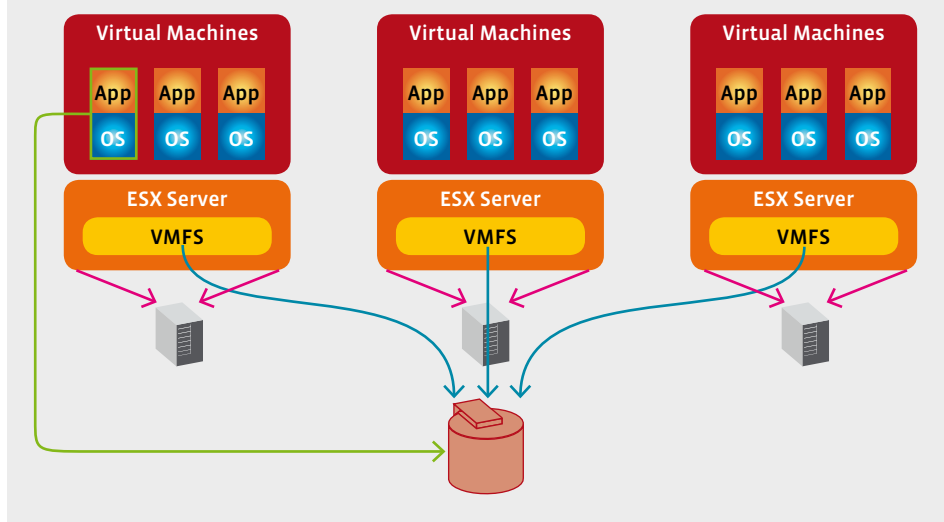
Oprogramowanie VMware Infrastructure transformuje zbiory różnych serwerów x86/x64 w zestawy logicznych zasobów umożliwiających przetwarzanie danych. Poszczególne systemy operacyjne oraz ich aplikacje zostają bezpiecznie odizolowane w przenośnych maszynach wirtualnych. Zasoby systemowe są następnie dynamicznie przydzielane poszczególnym maszynom wirtualnym według potrzeb i priorytetów. Każda maszyna wirtualna może zostać uruchomiona na dowolnym fizycznym serwerze wchodzącym w skład infrastruktury i każda z nich może zostać przeniesiona na inny serwer bez przerywania jej pracy. Pozwala to dynamicznie i automatycznie przenosić poszczególne maszyny wirtualne na te serwery, które są najbardziej odpowiednie dla zagwarantowania właściwego poziomu obsługi konkretnej aplikacji (SLA).

## Komponenty VMware Infrastructure

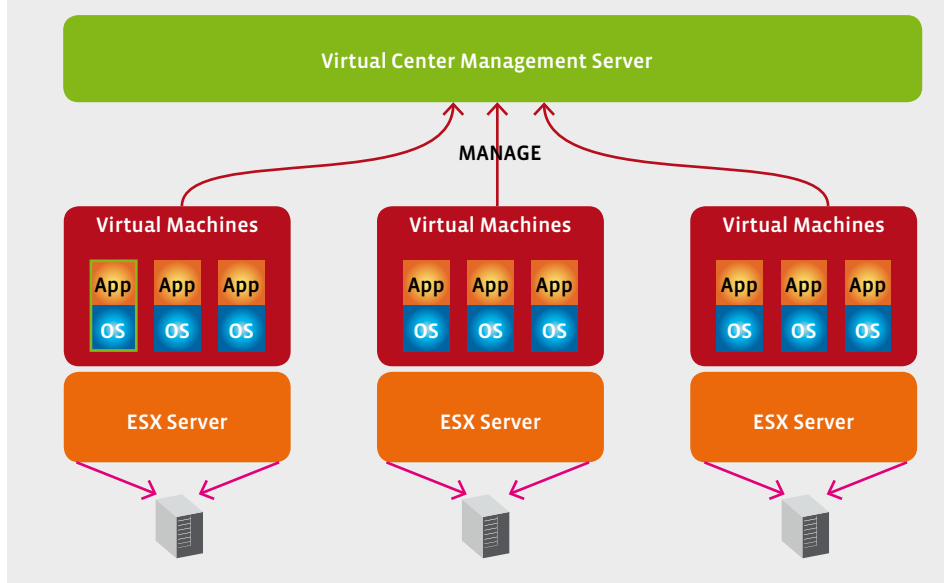
▶ **VMware ESX Server.** Działa na fizycznych serwerach, które udostępniają procesor, pamięć operacyjną, pamięć masową i zasoby sieciowe wielu wirtualnym maszynom w jednym momencie. Oprogramowanie ESX Server instaluje się bezpośrednio na fizycznym serwerze, który ma wnieść swoje zasoby do wirtualnej infrastruktury. ESX Server to solidna warstwa wirtualizacji, umożliwiająca fizycznemu serwerowi obsługę wielu maszyn wirtualnych, uruchamianych obok siebie w bezpieczny i przenośny sposób.

▶ **System plików VMFS firmy VMware.** Wysoko wydajny, klastrowy system plików przeznaczony dla maszyn wirtualnych. Maszyny wirtualne pozostają całkowicie zamknięte w swych plikach dyskowych, które mogą być przechowywane lokalnie na dyskach serwera lub centralnie we współdzielonej pamięci masowej w technologii SAN, NAS lub iSCSI. Klastrowy system plików umożliwia innowacyjne i unikatowe usługi, możliwe tylko dzięki wirtualizacji. Obejmują one przenoszenie pracujących maszyn wirtualnych

Rysunek 3. Komponenty VMware Infrastructure



Rysunek 4.



z jednego fizycznego serwera na inny serwer bez przerywania ich pracy, automatyczny restart maszyny wirtualnej po awarii jej serwera na jakimś innym fizycznym serwerze oraz łączenie w klastry maszyn wirtualnych uruchomionych na różnych fizycznych serwerach.

» **VMware Virtual SMP.** Moduł ten pozwala podnieść wydajność maszyny wirtualnej poprzez umożliwienie jej równoczesnego dostępu do wielu fizycznych procesorów goszczącego ją serwera fizycznego, okresowo przenosi zadania

między dostępnymi procesorami, aby zrównoważyć obciążenie. Pozwala to na wykorzystanie wirtualizacji także w odniesieniu do aplikacji najintensywniej wykorzystujących procesory, takich jak bazy danych, aplikacje ERP czy CRM.

» **VMware VirtualCenter.** VirtualCenter Management Server umożliwia centralne zarządzanie setkami hostów ESX Server i tysiącami maszyn wirtualnych, zapewnia funkcje automatyzacji czynności, optymalizacji zasobów i wysoką dostępność w środowiskach informatycznych.

Te możliwości gwarantują niespotykaną łatwość serwisowania, wydajność i niezawodność. Za jego pomocą maszyny wirtualne mogą być tworzone, konfigurowane, uruchamiane, zatrzymywane, usuwane czy przenoszone na inne serwery.

» **VMware DRS.** Oprogramowanie VMware Distributed Resource Scheduler (DRS) inteligentnie, dynamicznie przydziela i bilansuje moc obliczeniową dostępną na zbiorach zasobów sprzętowych, udostępniając ją maszynom wirtualnym. Moduł VMware DRS współpracuje z pakietem VMware Infrastructure, zajmując się ciągłym, automatycznym równoważeniem obciążeń poszczególnych maszyn wirtualnych pracujących w danej klastrze wirtualnej infrastruktury.

» **VMware VMotion.** Umożliwia przenoszenie maszyn wirtualnych z jednego fizycznego serwera na inny bez przerywania ich pracy (migracja „na żywo”), czyli z zachowaniem ciągłości działania usługi biznesowej. Ponadto moduł VMotion stale, automatycznie optymalizuje maszyny wirtualne danej puli zasobów dla uzyskania maksymalnego wykorzystania sprzętu, możliwe dużej elastyczności i dostępności.

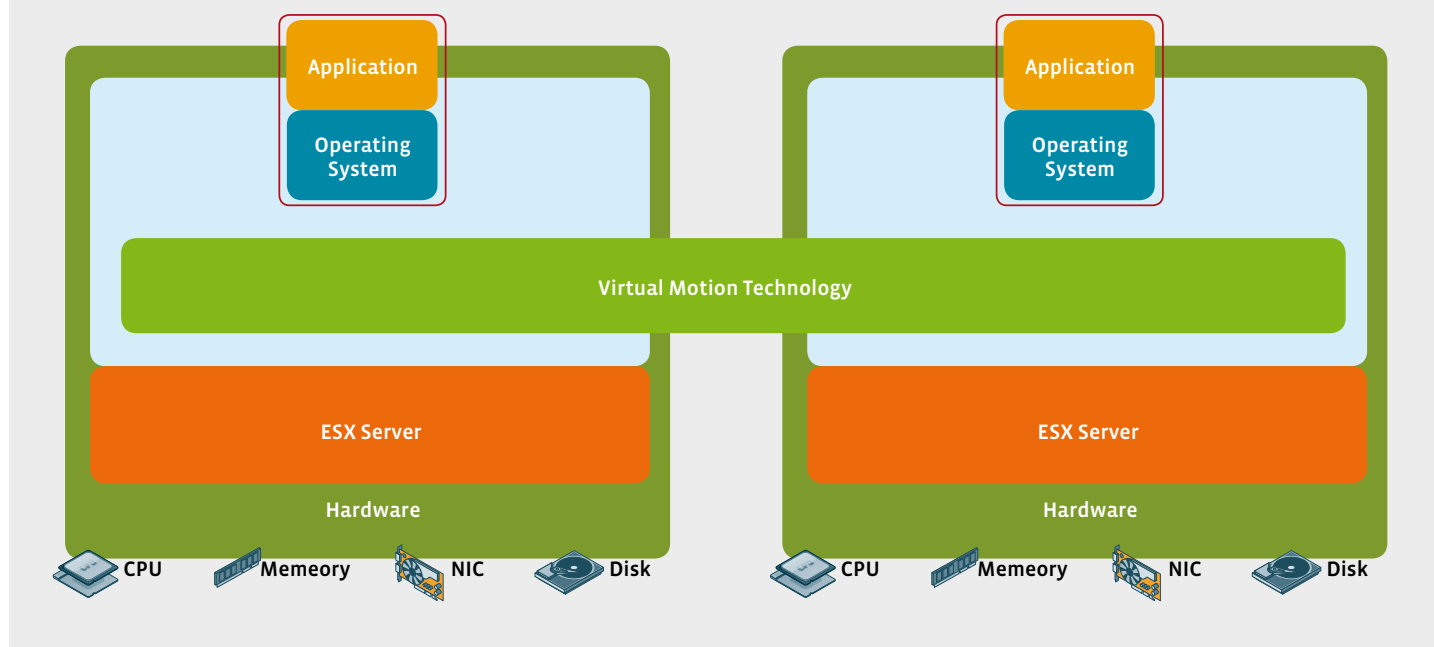
» **VMware HA.** Łatwe w użyciu, ekonomiczne rozwiązanie zapewniające wysoką dostępność aplikacji działających na maszynach wirtualnych. W przypadku awarii serwera maszyny wirtualne dotknięte awarią są automatycznie uruchamiane na innych serwerach eksploatacyjnych, dysponujących wolnymi zasobami.

» **VMware Consolidated Backup.** VMware Consolidated Backup to narzędzie do łatwego w użyciu, scentralizowanego tworzenia kopii zapasowych maszyn wirtualnych. Moduł VMware Consolidated Backup umożliwia poprzez centralnie zarządzane procedury backupu wykonywanie kopii zapasowych bez angażowania sieci produkcyjnej LAN i z zachowaniem wirtualnej struktury plików. Technologia ta doskonale integruje się z większością specjalizowanych, zewnętrznych narzędzi dla systemów backupowych (np. EMC/Legato NetWorker, VERITAS NetBackup, CA ARCserve).

## Nie wszystko jest takie różowe

Nie ulega wątpliwości, że dzięki wirtualizacji za podobne pieniądze można zapewnić większą niezawodność oraz szybsze reagowanie na pojawiające się sytuacje awaryjne. Poprzez odseparowanie poszczególnych aplikacji na dedykowanych dla nich serwerach zwiększa się ich stabilność, a także zyskuje możliwość oddzielenia użytkowników. Dzięki temu osobom odpowiadającym za bez-

Rysunek 5.



Miłosz Brzozowski

Comarch SA

**Stanowisko:** Konsultant ds. Outsourcingu  
Infrastruktury

**Sektor:** Usługi

Współautor: Paweł Albert

pieczeństwo w firmie przybędzie jedna dodatkowa warstwa ochronna w postaci hosta goszczącego środowiska wirtualne, ale i też – jedna warstwa, którą należałoby chronić. Wykraść dane z serwera bądź uruchomić złośliwe oprogramowanie można tak samo łatwo w przypadku serwera wirtualnego, jak do tej pory z fizycznej maszyny. A skuteczny atak może skończyć się uruchomieniem złośliwego serwera wirtualnego. Szkody mogą okazać się zatem dość znaczące. Administratorzy bezpieczeństwa powinni wykazać się podwójną czujnością.

Innego rodzaju problemy wiązać się będą na pewno z wydajnością środowisk wirtualnych. Większość firm korzystać będzie z maszyn wirtualnych ze znacznym narzutem obliczeniowym. Może to być źródłem problemów z niewydajną pracą systemów, aplikacji, w zvirtualizowanych środowiskach. Kolejne tworzone serwery wirtualne mogą pociągnąć za sobą przeciążenie hosta i w efekcie końcowym – problemy z zapanowaniem nad środowiskiem.

Najpoważniejszym jednak problemem jest znaczna koncentracja systemów w obrębie pojedynczej jednostki obliczeniowej, co czyni takie środowisko mocno podatnym na awarie. Awaria pojedynczego serwera (fizycznego) może wyłączyć całkiem pokaźną liczbę aplikacji biznesowych, niezbędnych do prawidłowego działania firmy. Zapewnienie niezawodności, redundancji i dynamicznego przełączania zasobów na wypadek awarii środowiska jest w takim razie absolutnie niezbędne, ale

skonsumuje część finansowych zysków z zastosowania wirtualizacji.

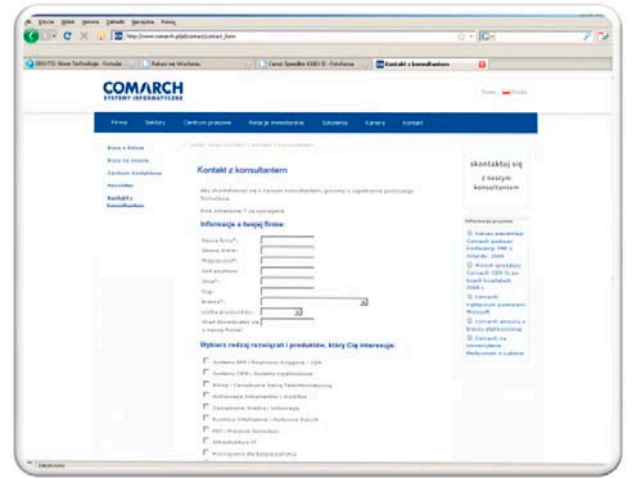
Osobna kwestia to swego rodzaju bariery mentalne przed przejściem na wirtualizację. Biznes i kadry zarządzające przyzwyczajone są do zakupów fizycznych zasobów, sprzętu, infrastruktury pod każdą nową aplikację. Procesy rozwoju firm i ich struktura organizacyjna dostosowane są do takiego właśnie scenariusza. Zyski wynikające z wirtualizacji są oczywiste dla działów IT, ale trudno je czasem wykazać w postaci konkretnych oszczędności. Występując z projektem oszczędnościowym, opartym na technologiach wirtualizacyjnych, należałoby zatem starannie i szczegółowo przygotować wykaz osiągniętych korzyści i wymiennie oszacować oszczędności.

### Technologia przyszłości? Wirtualizacja!

Jak każda nowa technologia wirtualizacja niesie ze sobą zarówno nowe możliwości, szanse, jak i obawy i zagrożenia. Jednak już na pierwszy rzut oka widać, że suma zalet przewyższa wszystkie niedostatki i potencjalne problemy. Czas i doświadczenie pozwolą zniwelować zagrożenia i zwiększyć szanse na osiągnięcie sukcesu. Dlatego już dziś warto pomyśleć o wdrożeniu wirtualizacji w swoim centrum danych. Przyszłość infrastruktury należy do świata zvirtualizowanego. Przyszłość należy do VMware.

# Chcesz otrzymywać magazyn Nowe Technologie za darmo w wersji papierowej bądź elektronicznej?

[www.comarch.pl/pl/contact/contact\\_form](http://www.comarch.pl/pl/contact/contact_form)



## Informacje o Twojej firmie:

Nazwa firmy: .....  
 Strona WWW: .....  
 Miejscowość: .....  
 Kod pocztowy: .....  
 Ulica: .....  
 Kraj: .....

Branża: .....  
 Liczba pracowników: .....  
 Skąd dowiedziałeś się o naszej firmie? .....

## Wybierz rodzaj rozwiązań i produktów, który Cię interesuje:

- |   |   |   |
|---|---|---|
| <input type="checkbox"/> Bankowość internetowa i usługi finansowe | <input type="checkbox"/> Rynki kapitałowe i instrumenty finansowe | <input type="checkbox"/> Systemy ERP i Finansowo-Księgowe – CDN |
| <input type="checkbox"/> CRM i zarządzanie sprzedażą              | <input type="checkbox"/> Procesy ubezpieczeniowe                  | <input type="checkbox"/> Zarządzanie Wiedzą i Informacją        |
| <input type="checkbox"/> Procesy kredytowe                        | <input type="checkbox"/> Rozwiązania dla bezpieczeństwa           | <input type="checkbox"/> Infrastruktura IT                      |

## Jakimi innymi rozwiązaniami jesteś zainteresowany(a):

.....  
 .....  
 .....

Proszę o kontakt telefoniczny

## Dane kontaktowe:

Imię: ..... Telefon: .....  
 Nazwisko: ..... Telefon komórkowy: .....  
 Stanowisko: ..... Fax: .....  
 E-mail: .....

Wyrażam zgodę na przetwarzanie moich danych osobowych (zgodnie z Ustawą z dnia 29.08.1997 r. o Ochronie Danych Osobowych, Dz.U. nr 733 poz. 883). Dane te będą wykorzystywane wyłącznie dla celów marketingowych i nie będą udostępniane innym podmiotom. Jednocześnie oświadczam, że zostałem poinformowany, iż mam prawo wglądu do swoich danych osobowych oraz możliwość ich poprawiania.

Data ..... Cytelny podpis .....

# Software as a Service (SaaS)

NOWE MOŻLIWOŚCI COMARCH DATA CENTER

system

Model SaaS, zdobywający coraz większą popularność na rynku rozwiązań IT, zachęca do zagłębienia się w jego istotę potencjalnymi możliwościami obniżenia kosztów TCO, podniesienia dostępności rozwiązania i innych korzyści wynikających z jego charakterystyki. Jak przedstawia się to z perspektywy Comarch Data Center?

## Historia

Oprogramowanie w formie usług, czyli SaaS, to ostatnio modny temat poruszany na łamach wielu magazynów zajmujących się tematyką IT. Przekora czy może wrodzony sceptycyzm nakazują mi zastanowić się nad istotą tego modelu biznesowego – czy opisywane szeroko korzyści to realna perspektywa, czy tylko mrzonka?

Skojarzenie nasuwające się ze świadczeniem usług tego typu „na żądanie” przywodzi na myśl dobrze znany model ASP (Application Service Provider), od którego rynek wydaje się oddalać, jeżeli nie porzucił go zupełnie już wcześniej. ASP, będące nierozdzielnie związane z architekturą klient-serwer i rozbitiem na dostawcę aplikacji (serwowanej jako jedna instancja per klient) oraz platformy sprzętowej, powoli traci na znaczeniu na korzyść SaaS – właśnie z powodu wspomnianego podziału. W modelu SaaS w idealnym położeniu znajdzie się producent aplikacji, posiadający możliwość dostosowania jej tak, aby możliwe było dzierżawienie na żądanie jej jednej instancji dla wielu klientów. Posiadanie infrastruktury, na której usadowiona będzie owa aplikacja w ramach tej samej organizacji, w pełni umożliwi czerpanie korzyści ze świadczenia usług zgodnie z filozofią „jeden dla wielu” (one-to-many, multi-tenant architecture).

Co ciekawe, już w 2006 roku ów model biznesowy cieszył się sporym zainteresowaniem, a struktura na ów czas według Forrester Research przedstawiała się tak, jak widać na rysunku 1:

Wydaje się, że wraz ze wzrostem wartości marketingowej pojęcia SaaS znacznie zmniejszyła się liczba respondentów wykazujących brak zainteresowania czerpaniem korzyści raczej z usługi niż z posiadania aplikacji na własność.

## Korzyści i zagrożenia wynikające z wykorzystania SaaS

Przedsiębiorstwo będące tzw. software house, świadczącym także usługi w innych obszarach IT, nie pomijając szczególnie istotnych – w świetle interesującego nas zagadnienia – usług Data Center, może potencjalnie być zainteresowane modelem SaaS lub przynajmniej niektórymi jego aspektami. Dzieje się tak, ponieważ w ramach jednej firmy skupiają się nie tylko wszystkie elementy wymagane do tego, aby skutecznie sprzedawać oprogramowanie jako usługę, ale także możliwość łączenia tego z wykorzystaniem wysoko dostępnej, wydajnej i wyskalowanej „pod rozwiązanie” architektury fizycznej. Bliskość i wynikająca z niej możliwość efektywnej wymiany informacji pomiędzy departamentami piszącymi produkty software a działem data center powoduje, że możliwe jest stworzenie wydajnych, wysoko dostępnych plat-



form SaaS. Platformy owe będą spełniać formalne założenia modelu sprzedaży oprogramowania jako usług, a poprzez to zapewniać wysoką dostępność, wydajność i obniżenie kosztu licencji oraz hardware'u (poprzez konsolidację w warstwie logicznej i fizycznej). Poza kosztem fizycznych urządzeń łatwo wyobrazić sobie korzyści płynące z licencjonowania baz danych, systemów operacyjnych i innych składników software znajdujących się poniżej warstwy samej aplikacji, jeżeli mamy do czynienia z tylko jedną instancją dla wielu korzystających. Przykładem może być sytuacja, kiedy wielu klientów płaci za dostęp do tej samej bazy danych licencjonowanej w modelu per procesor – przy tradycyjnym rozwiązaniu koszt licencji w całości spoczywa na pojedynczym kliencie, tu jednak rozkłada się na wielu, a liczba użytkowników ograniczona jest jedynie wydajnością sprzętu. Nie bez znaczenia z tej perspektywy jest także wyeliminowanie problemów z niespójnościami powstającymi nieraz podczas prób raportowania danych pochodzących z różnych wersji aplikacji – teraz software zawsze będzie aktualny.

SaaS, mocno związany z ideą outsourcingu niektórych obszarów działalności przedsiębiorstw, zakłada oddanie w ręce usługodawcy pewnego zakresu działalności czy procesu biznesowego. Oznacza to oczywiście zrzucenie odpowiedzialności na dostawcę rozwiązania, co może być postrzegane jako korzyść, ale spotyka się także ze sceptycyzmem w przypadku bardziej wymagających potencjalnych klientów. Sceptycyzm ów jest tym większy, im cenniejsze są dla nich dane i im bardziej krytyczna jest bezwarunkowa dostępność

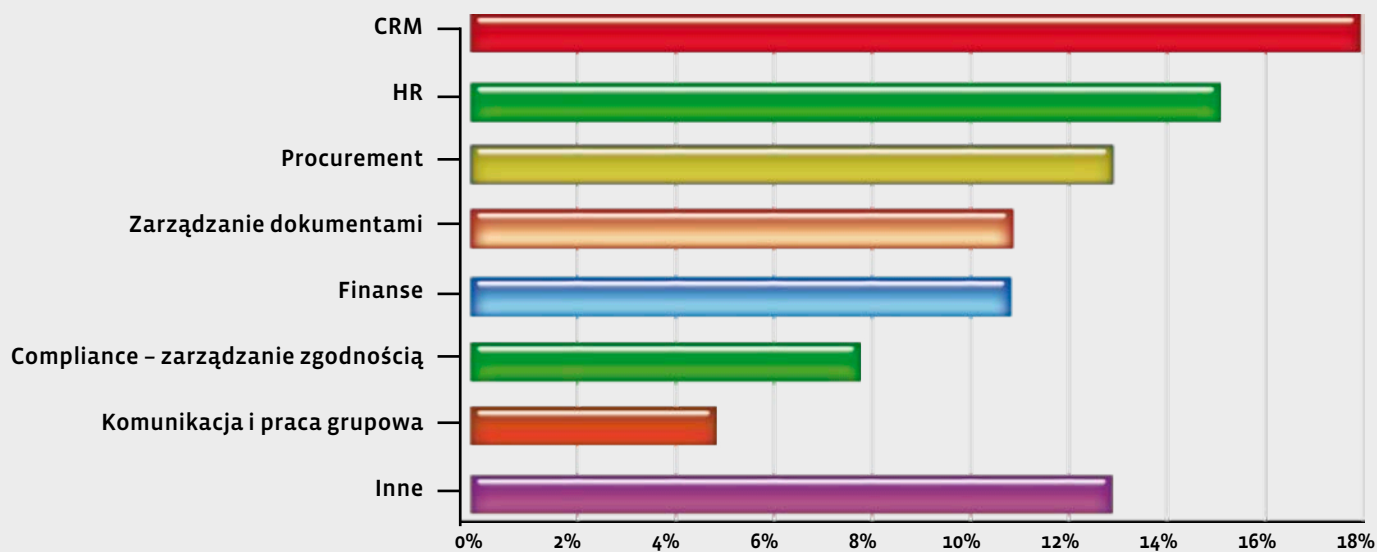
rozwiązania. Między innymi z tego powodu obecnie SaaS cieszy się dużą popularnością wśród mniejszych i średniej wielkości firm, zatrudniających od 10 do około 50 osób. Takie przedsiębiorstwa mogą potencjalnie przykładać większą uwagę do korzyści finansowych płynących z zastosowania oprogramowania udostępnianego jako usługa za pośrednictwem przeglądarki WWW.

Wśród czynników postrzeganych jako najważniejsze, jeżeli chodzi o zainteresowanie rozwiązaniami SaaS, przoduje uproszczenie zarządzania aplikacją, redukcja kosztów operacyjnych i prawie w tym samym stopniu przyspieszenie czasu implementacji oraz zwiększenie poziomu umów serwisowych.

Według Gartnera, użycie oprogramowania w formie usług w zależności od obszaru zastosowań miało w 2007 roku strukturę przedstawioną na schemacie na następnej stronie.

## SaaS w CDC – konsolidacja warstwy logicznej a hardware

Korzystanie z jednej instancji aplikacji dla wielu klientów to nie jest jedyny obszar konsolidacji, jeżeli rozpatrujemy udostępnianie software'u jako usług. Podobna sytuacja dotyczyć będzie wszystkich warstw architektury rozwiązania zarówno w ujęciu logicznym, jak i fizycznym. Konsolidacja zakładająca wspólne korzystanie z serwerów aplikacji, baz danych i platform sprzętowych to – poza rezygnacją z modelu klient-serwer na rzecz korzystania z aplikacji za pośrednictwem przeglądarki – nieodłączne elementy filozofii SaaS. Nietrudno wyobrazić sobie, że przypisanie większej niż 1 liczby klientów

**Rysunek 2. Użycie aplikacji jako usług w podziale na rodzaj oprogramowania**

do jednego serwera, zasobu dyskowego i innych elementów infrastruktury kosztuje mniej niż rozwiązania dedykowane. Przytoczony przykład znacznie upraszcza faktyczny stan rzeczy, jednak wciąż jest prawdziwy. W rzeczywistości sfera fizyczna sprowadzi się do wykorzystania wspólnych dla jednej aplikacji farm serwerów w ramach wszystkich warstw, scentralizowanych zasobów dyskowych dających się dzielić na mniejsze części przypisywane do poszczególnych klientów, centralne



### Jakub Pysz

#### Comarch SA

**Stanowisko:** Konsultant Comarch Data Center

**Sektor:** Usługi/Infrastruktura

**Info:** Specjalizuje się w projektowaniu wielowarstwowych, korporacyjnych rozwiązań IT

systemy backupu i inne elementy infrastruktury wykorzystywane przez wielu usługobiorców na raz. Infrastruktura roznosi się w umiarkowanym tempie, jeżeli chodzi o jej rozmiary fizyczne, a i inżynierowie data center trzymający pieczę nad sprzętem mogą poświęcić więcej uwagi rozwiązaniu skupiającemu wielu klientów. Zespół inżynierów nie będzie również roznosić się tak szybko jak liczba inżynierów systemowych i atencja wymagana przez coraz większą liczbę maszyn, systemów operacyjnych, serwerów aplikacji czy instancji baz danych. Z punktu widzenia dostawcy usług data center oznacza to oczywiście użycie odpowiednio wydajnych maszyn: pojemnych, szybkich i – dla wszystkich elementów infrastruktury – wysoko dostępnych i skalowanych rozwiązań. Naturalną refleksją jest to, że niedostępność systemu hostującego rozwiązanie w modelu SaaS jest równoznaczna z zatrzymaniem świadczenia usługi nie dla jednego, lecz dla wielu klientów. W istocie – poniekąd paradoksalnie – oznacza to korzyść dla usługobiorcy, ponieważ świadczący usługę SaaS po prostu nie może pozwolić sobie w takim układzie na stosowanie rozwiązań kompromisowych, tanich czy posiadających wiele tzw. single points of failure.

### Wnioski i podsumowanie

SaaS z perspektywy infrastruktury to rozwiązanie szczególnie zasługujące na uwagę przede wszystkim mniejszych (lecz nie tylko!) przedsiębiorstw i specyficznych obszarów ich działalności, dlatego daleki jestem od bezkrytycznego zachwalania wszystkich cech takiego modelu biznesowego w kontekście wszystkich klientów i usług IT. Idea oprogramowania jako usługi nie zawsze sprost

wymaganiom firm dużych, których dane stanowią krytyczny element biznesu, a obawa przed ich dostaniem się w niepowołane ręce to najważniejszy ze wszystkich czynników polityki bezpieczeństwa. Nie musi to oczywiście oznaczać, iż nie ma obszarów działalności w klasie enterprise, w których podejście SaaS przyniosłoby wiele pożytku. Korzyści cenowe wynikające z konsolidacji w obrębie wszystkich warstw architektury, a zarazem ten sam poziom jakości usług co przy rozwiązaniach dedykowanych dla poszczególnych klientów wydają się mówić same za siebie. Najważniejsze jednak jest to, aby pamiętać, iż nie jest to rozwiązanie uniwersalne, a udane wdrożenie w modelu SaaS będzie uzależnione przede wszystkim od prawidłowo wykonanej analizy w sferze języka i logiki biznesu, a dopiero potem w kwestii technologicznej.

Comarch jako producent aplikacji, integrator, a także dostawca usług data center zbliża się do modelu SaaS przynajmniej w przypadku kilku swoich produktów. Jeżeli nie jest to czyste w formie podejście SaaS, to przynajmniej część filozofii znajduje zastosowanie w przypadku wielu produktów software dostępnych za pośrednictwem Comarch Data Center. W modelu, w którym oprogramowanie jest w zasadzie usługą udostępnianą na żądanie w duchu SaaS, znajdują się przykładowo produkty ECOD, takie jak Operator, Data Share czy Archiwum, działające za pośrednictwem przeglądarki WWW. Usługi te udostępniane są zgodnie z modelem SaaS za pośrednictwem jednej instancji aplikacji, bazy danych i wspólnej architektury fizycznej. Planowana jest również sprzedaż innych produktów jako usług, dotyczy to m.in. rodziny aplikacji Comarch Loyalty Management.



# Dostęp satelitarny – wczoraj, dziś i jutro

**HISTORIA** telekomunikacji satelitarnej zaczęła się w październiku 1945 r. Wówczas to w brytyjskim magazynie „Wireless World” były oficer Królewskich Sił Powietrznych **Arthur Charles Clarke** opublikował artykuł naukowy pt. „Extra-terrestrial Relays”, w którym zawarł ideę wykorzystania satelitów umieszczonych na orbitach geostacjonarnych do stworzenia światowej sieci łączności.

Clarke przewidywał, że odpowiednio rozmieszczone 3 satelity będą w stanie zapewnić ludziom z całego świata możliwość komunikowania się. Studium to uznano wówczas za wizję fantasty, jednak z czasem dało ono podwaliny pod dzisiejszą technikę satelitarną. Kolejnym kamieniem milowym było wystrzelenie 4 października 1957 r. przez ZSRR pierwszego sztucznego satelity Ziemi – Sputnika 1. Przez ponad 50 lat od wystrzelenia Sputnika na orbicie pojawiły się tysiące jego następców. W roku 2005 znajdowało się tam już 536 funkcjonujących satelitów telekomunikacyjnych (z czego 298 na orbicie geostacjonarnej). Szacuje się, że w latach

2006-2015 kolejnych 176 satelitów zostanie wyniesionych na orbitę geostacjonarną.

Obecnie telekomunikacja satelitarna to najbardziej dochodowy segment rynku usług satelitarnych. Wartość rynku związanego z przestrzenią kosmiczną i odpowiednimi zastosowaniami wynosi w skali światowej około 70 mld euro i rynek ten rośnie w tempie około 7 proc. rocznie.

## Gdzie WiMax nie może...

Czy dostęp satelitarny do sieci w czasach powszechnego niemal szerokopasmowego dostępu do Internetu ma sens? Czy w czasach dynamicznego rozwoju usług bezprzewodowych, takich jak WiMax czy UMTS, dostęp satelitarny stanowi jakąś alternatywę? Paradoksalnie, rynek ten rozwija się coraz bardziej dynamicznie, a najbardziej dynamiczny wzrost jest oczekiwany w dziedzinie interaktywnych usług szerokopasmowych – transmisji danych i video, radia cyfrowego i regionalnych systemów mobilnych. Choć udział segmentu satelitarnego w całości wolumenu światowych transmisji tele-

komunikacyjnych nie przekracza 5 procent, znaczenie przekazu dokonywanego za pomocą satelitów komunikacyjnych jest kluczowe dla gospodarczego i cywilizacyjnego rozwoju społeczeństw i państw, a możliwości oferowane przez te techniki są trudne do zastąpienia. Jednym z istotnych czynników rozwoju łączności satelitarnej w ciągu kilkunastu najbliższych lat będzie wzrost zapotrzebowania na usługi szerokopasmowe, przy czym zakłada się, że zwiększony popyt widoczny będzie głównie po stronie użytkowników instytucjonalnych. Satelitarne systemy szerokopasmowe służyć będą jako uzupełnienie systemów naziemnych (światłowodowych i radiowych), pozwalając na zapewnienie usług łącznościowych użytkownikom nieposiadającym dostępu do sieci naziemnych.

Trzeba jednak podkreślić, że rozwiązania satelitarne ze względu chociażby na cenę nigdy nie będą rozwiązaniami masowymi. Obecnie rozwój technologii bezprzewodowych, takich jak WiMax, WiFi czy HSDPA, powoduje, że w dużych skupiskach ludności stosowanie rozwiązań satelitarnych będzie

ekonomicznie nieuzasadnione. Duże koszty emisji satelitarnych, relatywnie małe przepływności i efektywności widmowe oraz duże opóźnienia w transmisji powodują, że powszechny dostęp do sieci Internet z wykorzystaniem satelitów geostacjonarnych, zarówno jednokierunkowy, jak i dwukierunkowy, nie stanowi alternatywy dla przyszłych sieci naziemnych. Technologia satelitarna nie jest skierowana na rynek klienta masowego.

Natomiast w kilku przypadkach wydaje się bezkonkurencyjna:

- » łącza zapasowe dla klientów instytucjonalnych,
- » dostęp do sieci na obszarach słabo rozwiniętych,
- » dostępy okazjonalne.

W przypadku łączy backupowych satelitarne systemy szerokopasmowe stosuje się jako uzupełnienie systemów naziemnych (światłowodowych i radiowych), zapewniając łączność użytkownikom nieposiadającym dostępu do sieci naziemnych, np. w przypadku awarii. Wypada zwrócić uwagę na to, że praktycznie cała trasa transmisyjna przebiega poza infrastrukturą naziemnych operatorów funkcjonujących w danym kraju. Oznacza to, że nawet w wypadku awarii sieci szkieletowej mamy możliwość korzystania z dostępu do sieci. Jesteśmy całkowicie niezależni od krajowych operatorów – czy to przewodowych, czy też bezprzewodowych. Punkt styku z Internetem mieści się daleko poza granicami kraju, co powoduje, że jest skutecznie odseparowany od wszystkich awarii mogących trafić operatorów stacjonarnych. Dodatkowym czynnikiem jest kwestia bezpieczeństwa i jakości transmisji. Na potrzeby połączenia zostaje stworzony szyfrowany kanał z gwarantowanym pasmem.



**Michał Szybalski**

Comarch SA

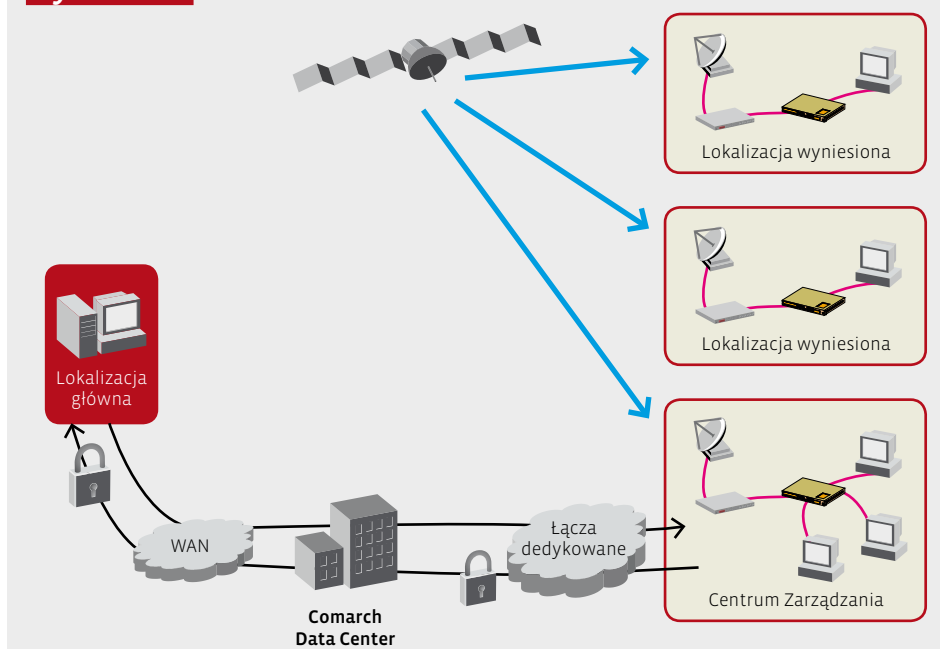
**Stanowisko:** Business Solution Manager

**Sektor:** Usługi

**Info:** W Comarch SA zajmuje się m. in. kwestiami przesyłu danych i głosu, sieciami LAN i WAN oraz rozwiązaniami Call i Contact Center

nowe technologie [magazyn comarch]

**Rysunek 1.**



W przypadku projektów wdrożonych przez Comarch z reguły stosujemy infrastrukturę w pełni redundantną.

Dzięki temu, że obieg danych wygląda w sposób następujący: komputer w lokalizacji oddalony – stacja nadawcza – stacja odbiorcza – Comarch Data Center – lokalizacja główna klienta, zapewniana jest pełna poufność danych przy redukcji do minimum czasu transmisji.

Drugą dziedziną, w której ma zastosowanie transmisja satelitarna, jest dostęp dla lokalizacji znajdujących się na obszarach słabo rozwiniętych telekomunikacyjnie. Internet dostarczany drogą satelitarną stanowi tu często jedyne efektywne technicznie i kosztowo rozwiązanie. W szczególności może to dotyczyć rejonów górskich, ale i np. stacji benzynowych położonych poza miastami, z daleka od tras telekomunikacyjnych. Rozwiązania satelitarne są bardzo popularne w segmencie sieci stacji paliw. W Polsce, często za pośrednictwem Comarch, z tego rodzaju transmisji korzysta w całości (np. Lotos, Shell, Neste) lub części (np. BP, Statoil) większość z nich.

Dostępy okazjonalne (ad hoc) wykorzystują nieograniczoną wręcz mobilność, na jaką pozwala nam technologia satelitarna. Pierwotnym beneficjentem tego rodzaju rozwiązań była telewizja. Usługi SNG (Satellite News Gathering) swoje początki datują w czasach konfliktu brytyjsko-argentyńskiego o Falklandy. Wykorzystywano wówczas analogową transmisję satelitarną. Rozkwit usług SNG przypada jednak na czas pierwszej interwencji w Iraku. Wówczas to masowo pojawiły się systemy wykorzystujące transmisję cyfrową, pozwalające nadawać z dowolnego miejsca i szybko zmieniać położenie.

Obecnie z dostępu okazjonalnych korzysta nie tylko telewizja. Jest to np. idealne narzędzie dla służb zarządzania kryzysowego. W USA w 2005 roku po ataku huraganu Katrina na obszarze kłęski pracowało kilkadziesiąt tysięcy satelitarnych telefonów sieci Iridium i Globalstar, tworząc efektywny system łączności funkcjonujący przez kilka tygodni po katastrofie.

## Przyszłość rozwiązań satelitarnych

Jak będzie wyglądała przyszłość takich systemów? Rozwiązania satelitarne będą funkcjonować jako rozwinięcie lub uzupełnienie „tradycyjnych” metod transmisji danych oraz dostępu do Internetu. VSAT znajdzie swoje miejsce wszędzie tam, gdzie należy zestawić transmisję szybko i niezawodnie, gdzie wymagana jest mobilność rozwiązania oraz niezależna od infrastruktury lokalnej transmisja zapasowa. Mariaż tych technologii naziemnych (przewodowych i bezprzewodowych) oraz satelitarnych pozwala zwykle na znaczne przyspieszenie czasu uruchomienia usługi oraz obniżenie sumarycznych kosztów wdrożenia i eksploatacji.

Kto może być użytkownikiem takich usług? Od instytucji finansowych, poprzez usługi pocztowe i kurierskie, samorządy, sieci sprzedaży, firmy budowlane, aż po służby mundurowe.

Jak stwierdziła Viviane Reding, komisarz UE odpowiedzialna za telekomunikację: *Potencjał ogólnoeuropejskich satelitarnych usług komunikacji ruchomej jest ogromny – wystarczy pomyśleć o telewizji komórkowej, ogólnodostępnych łączach szerokopasmowych, ochronie ludności czy pomocy w przypadku katastrof.*

# Bezpieczeństwo Twoich danych to zadanie dla profesjonalistów

## Comarch Rozwiązania dla bezpieczeństwa:

- Comarch Security Access Manager
- Comarch Mobile Security
- Comarch PKI
- Comarch CentralLog
- Comarch SecureAdmin
- Comarch SafeDesktop



Zobacz więcej na:

[www.finance.comarch.pl](http://www.finance.comarch.pl)

**COMARCH**  
SYSTEMY INFORMATYCZNE

← Intro

Aktualności | Opracowania | **0-801 334455**

01 | 12 | 2008 **Comarch Debt Management w Allianz Banku**

Comarch zawarł z Allianz Bankiem umowę na wdrożenie systemu do windykacji wierzytelności Comarch Debt Management. System ten od czterech lat z powodzeniem funkcjonuje w spółkach ubezpieczeniowych grupy Allianz. Projekt wdrożeniowy obejmuje pełną funkcjonalność systemu oraz wysoki stopień automatyzacji działań, co pozwoli na szybką i skuteczną realizację procedur windykacyjnych.

- Rozwiązania Comarch dla ubezpieczeń
- Oddziały bez kolejek
- Fuzja z Comarch NonLife

Newsletter

adres e-mail

Case study

Fuzja dwóch Towarzystw Ubezpieczeniowych – UNIQA i FILAR SA jest niewątpliwie dużym wyzwaniem. Wybór systemu Com arch NonLife Insurance okazał się sukcesem.



**Life Insurance**

System Com arch Life Insurance jest kompleksowym rozwiązaniem informatycznym przeznaczonym dla firm ubezpieczeniowych. System został zaprojektowany z uwzględnieniem dominujących tendencji występujących na rynku ubezpieczeń. Przy tworzeniu systemu szczególną uwagę zwrócono na kwestię elastyczności wdrażania.

Należy do:

- Life Insurance
- NonLife Insurance
- Health Insurance
- Person
- Insurance Claims
- Commission and Incentive
- Insurance Fee
- Internet Insurance
- CRM Sales Management

**Opracowania**

- Rozwiązania Comarch dla ubezpieczeń
- Oddziały bez kolejek
- Fuzja z Comarch NonLife

Case study

Fuzja dwóch Towarzystw Ubezpieczeniowych – UNIQA i FILAR SA jest niewątpliwie dużym wyzwaniem. Wybór systemu Com arch NonLife Insurance okazał się sukcesem.

0-801 334455

Aktualności

01 | 12 | 2008 **Comarch Debt Management w Allianz Banku**

Comarch zawarł z Allianz Bankiem umowę na wdrożenie systemu do windykacji wierzytelności Comarch Debt Management. System ten od czterech lat z powodzeniem funkcjonuje w spółkach ubezpieczeniowych grupy Allianz.

01 | 12 | 2008 **Comarch Asset Management w OTP Capital**

Comarch zawarł z OTP Capital umowę na wdrożenie systemu do zarządzania aktywami Comarch Asset Management. System ten od czterech lat z powodzeniem funkcjonuje w spółkach ubezpieczeniowych grupy Allianz.

01 | 12 | 2008 **Comarch ubezpieczenia współprac z L&K LIFE**

Comarch zawarł umowę na wdrożenie systemu do zarządzania aktywami Comarch Asset Management. System ten od czterech lat z powodzeniem funkcjonuje w spółkach ubezpieczeniowych grupy Allianz.

01 | 12 | 2008 **Comarch Debt Management dla Uniwersalnego Towarzystwa Ubezpieczeniowego Komarny do Wzrostu**

Uniqa, które w ramach swojej działalności prowadzi działalność ubezpieczeniową oraz działalność Comarch Debt Management okazał się sprawna również jako poddawany system dla spółek windykacyjnych – dostaje Maciej Milewicz, Product Manager Comarch.

Allianz Bank jest nowo stworzonym bankiem na rynku polskim. Należy on do międzynarodowej grupy Allianz, która dzięki przetestowanym rozwiązaniom oferuje wysokie standardy obsługi. Dotychczasowo Grupa Allianz w Polsce tworzyła

**Opracowania**

- Rozwiązania Comarch dla ubezpieczeń
- Oddziały bez kolejek
- Fuzja z Comarch NonLife

Case study

Fuzja dwóch Towarzystw Ubezpieczeniowych – UNIQA i FILAR SA jest niewątpliwie dużym wyzwaniem. Wybór systemu Com arch NonLife Insurance okazał się sukcesem.

0-801 334455

Newsletter

# www.ubezpieczenia.comarch.pl

## Dowiedz się więcej na temat rozwiązań dedykowanych wyłącznie dla ubezpieczeń.