Komunikacja w czasie rzeczywistym – najnowszy biznesowy „must have”

Rynek komunikacji w czasie rzeczywistym tzw. Web RTC do 2017 roku przekroczy miliard dolarów. Według prognoz firmy analitycznej Markets&Markets jego dynamika nie zwolni i do 2022 roku rynek osiągnie wartość 6,5 mld dolarów przy rocznym wzroście około 44 proc. Szybkie tempo umożliwi technologia chmury.

Paweł **Pierścionek**

chief technology officer w Cludo

Komunikacja w czasie rzeczywistym, czyli Web RTC, to przybierający na sile biznesowy trend. Coraz chętniej sięgają po nią nie tylko największe korporacje, ale również firmy z sektora MSP, takie jak placówki medyczne, biura podróży czy sklepy internetowe. Dlaczego? Bo w dzisiejszym biznesie liczy się tu i teraz.

Biznes potrzebuje czasu… rzeczywistego

O komunikacji nie sposób mówić wyłączając filtr otoczenia, a zważywszy na liczbę istniejących obecnie kanałów, obejmujących wiadomości tekstowe, głos i video, klasyczny podział na komunikację werbalną i niewerbalną coraz trudniej odnieść do współczesnej rzeczywistości. To dzięki technologiom komunikacja na przestrzeni lat weszła na zupełnie inny poziom. Z jednej strony liczba wysyłanych komunikatów poprzez mail, telefon, aplikacje i inne komunikatory mocno wzrosła, z drugiej stały się one znacznie „płytsze”, a tempo wymiany informacji przyspieszyło. Przyzwyczailiśmy się do tego, że mamy możliwość kontaktowania się z kim chcemy i kiedy chcemy, a odpowiedź na ogół nadchodzi w ciągu kilku minut. Nic więc dziwnego, że zmiana sposobu komunikacji w pewnym sensie wymusiła również zmianę w podejściu do jej roli w biznesie. Można zaobserwować, że obecnie na rynku rośnie zainteresowanie narzędziami do ujednoliconej komunikacji, takimi jak platformy UCaaS i Web RTC. Przedsiębiorstwa coraz wyraźniej zauważają potrzebę inwestycji w profesjonalne systemy do zarządzania komunikacją zarówno wewnątrz swoich struktur, jak i do zewnętrznych kontaktów z klientami. Wbrew pozorom inwestycjami zainteresowani są nie tylko najwięksi rynkowi gracze, ale również firmy z sektora MSP i najmniejsze przedsiębiorstwa – podkreśla ekspert.

Ten trend potwierdzają również wyniki międzynarodowych badań Markets&Markets, zgodnie z którymi sprzedaż rozwiązań UCaaS (Unified Communication as a Service) wzrośnie w ciągu 5 najbliższych lat o 12 mld dolarów, a rynek komunikacji w czasie rzeczywistym tzw. Web RTC osiągnie wartość 6,5 mld dolarów. Jak oceniają eksperci, rynki napędzane są głównie przez technologie chmurowe, które stosunkowo niskimi kosztami wdrożeń zachęcają przedsiębiorców do inwestycji.

Stać Cię na dobre kontakty

To właśnie dzięki wykorzystaniu najnowszych rozwiązań z zakresu IT, w tym cloud computingu, narzędzia do komunikacji w czasie rzeczywistym są dostępne jako część większej całości oprogramowania w modelu UCaaS i mogą być dystrybuowane jako usługa i składowa całego systemu. W skład UCaaS wchodzą takie elementy, jak: komunikacja tekstowa, zarządzanie obecnością czy też narzędzia pracy grupowej, jak chociażby współdzielenie pulpitów. Na przystępność rozwiązań z tej kategorii znacznie wpływa również fakt wyeliminowania kosztów inwestycyjnych i szybkość wdrożenia usługi. Ponadto technologia chmurowa zapewnia elastyczność, co oznacza, że firma rozliczana jest za tyle licencji, ile faktycznie potrzebuje, w każdej chwili mogąc dowolnie regulować ich ilość, co znacznie ogranicza ryzyko inwestycyjne. Oszczędności są znaczące, bo firma decydująca się na chmurową platformę do komunikacji może zaoszczędzić nawet milion złotych w stosunku do wdrożenia centrali telefonicznej w modelu stacjonarnym na sto stanowisk, a dodatkowo zyskuje możliwość modyfikacji liczby potrzebnych licencji. Ma to szczególne znaczenie w przypadku najmniejszych odbiorców usługi, którzy często nie są w stanie dokładnie oszacować swoich potrzeb i nie wiedzą, jak w dłuższej perspektywie będzie rozwijał się ich biznes. Chmura jest receptą na te obawy.

Potencjał rynku jest ogromny, ponieważ jak szacuje IDC, do 2020 r. już co najmniej 45 proc. oprogramowania oraz infrastruktury informatycznej w europejskich przedsiębiorstwach będzie dostarczane w modelu chmurowym. Tym samym, w 2020 r. inwestycje w rozwiązania chmurowe będą stanowiły 20 proc. wydatków na infrastrukturę IT oraz 25 proc. wydatków przeznaczanych na zakup oprogramowania, usług i sprzętu. O zyskującym na znaczeniu trendzie świadczy również fakt, że obecnie coraz trudniej jest znaleźć producenta oprogramowania, którego rozwiązania nie są oferowane w modelu cloud. Prawdę powiedziawszy w branży contact center na przestrzeni ostatnich dwóch lat nie znam przypadku, w którym klient dokonujący wyboru rozwiązania pominąłby w swoich rozważaniach oferty systemów hostowanych.

Przemiany społeczne napędzają rynek rozwiązań RTC

Warto wspomnieć, że na rozwój rynku zintegrowanej komunikacji w czasie rzeczywistym wpływają również przemiany społeczne, które zaobserwować można zarówno w obsłudze klienta, jak i w modelu pracy coraz liczniejszej grupy społecznej, jaką są millenialsi – pokolenia wychowywane na technologii i przyzwyczajone do komunikacji „tu i teraz”. Ich przedstawiciele zarówno jako pracownicy, jak i klienci bardzo szanują swój prywatny czas, oczekują zainteresowania, szybkiej informacji zwrotnej i indywidualnego podejścia. Nie powinien więc dziwić fakt, że firmy zainteresowane są narzędziami, które umożliwiają realizację tych potrzeb.

Dla przykładu, rozwój technologii sprawił, że obecnie pracownik wcale nie musi przebywać w biurze żeby efektywnie wykonywać swoje obowiązki, bo może skorzystać z platformy komunikacyjnej, do której ma dostęp online. Wdrażane obecnie systemy do zarządzania komunikacją umożliwiają dostęp do firmowych zasobów z poziomu przeglądarki WWW. Tym samym np. konsultant czy handlowiec mogą obsługiwać swoich klientów o dowolnej godzinie i z dowolnego miejsca dysponując informacjami na temat poprzednich kontaktów, etapu załatwianej sprawy czy procesu sprzedażowego. Korzyści są dwojakie, bo z jednej strony pracownicy mogą elastycznie realizować swoje obowiązki, a z drugiej strony idea komunikacji w czasie rzeczywistym jest spełniona.

BIZNES RAPORT
GAZETA FINANSOWA
14–27 lipca 2017 r.

Bezpieczeństwo coraz większym wyzwaniem dla firm

W obecnych czasach, kwestia bezpieczeństwa w IT nie jest już zagadnieniem marginalnym. Wprost przeciwnie – cyberataki generują coraz większe straty dla firm, a dla przestępców są doskonałym źródłem pozyskania pieniędzy. Przedsiębiorcy, którzy inwestują w nowe technologie, powinni zdawać sobie sprawę z tego, że są narażeni na wszelkie zagrożenia związane z tym sektorem. Co powinni zrobić, żeby odpowiednio zabezpieczyć swoją firmę przed konsekwencjami cyberataków?

Maciej **Pokrzywiński**
dyrektor generalny IT Company

Coraz częściej w środowisku IT dochodzi do ataków złośliwego oprogramowania typu ransomware.

Ostatnie wydarzenia skłaniają do przemyśleń

Jest to rodzaj wirusa, za pomocą którego hakerzy przejmują kontrolę nad komputerem i ograniczają lub całkowicie uniemożliwiają korzystanie z niego – dopóki nie otrzymają żądanego okupu. Nie tak dawno w branży głośnym echem odbiła się sprawa ataku systemu tego typu, czyli WannaCry. Zainfekowanych zostało ponad 200 000 komputerów na całym świecie. W ostatnich dniach mamy do czynienia z kolejną wersją wirusa: Petya. Oprogramowanie atakuje nawet urządzenia, które zostały uzupełnione o wszelkie poprawki systemu Windows i powinny być wzmocnione po WannaCry. Wszelkie dowody wskazują na to, że celem ataku Petya nie było wyłudzenie okupów, ale zniszczenie firmowych danych. Chociaż ataki początkowo dotknęły głównie Ukrainę, to już wiadomo, że nie oszczędzą urządzeń w innych państwach, w tym także w Polsce. Szczególnie tych firmowych, ponieważ Petya upodobała sobie oprogramowania przedsiębiorstw. W naszym kraju, podobnie jak na świecie, wirus zaatakował głównie firmy z branży logistycznej, ale również mniejsze spółki usługowo-handlowe. A to może być dopiero początek.

Lepiej zapobiegać, niż leczyć

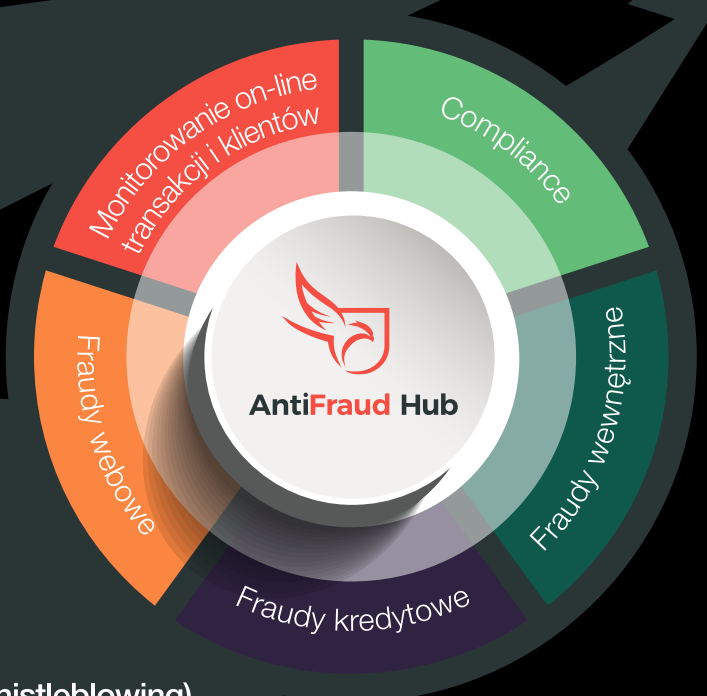
Zapewnienie odpowiednich środków bezpieczeństwa, chroniących przed atakami nie powinno być traktowane, jako dodatkowa opcja, którą można mieć, ale jako niezbędny element strategii biznesowej firmy. Niestety wciąż mamy do czynienia z sytuacją, w której wielu przedsiębiorców interesuje się kwestią bezpieczeństwa dopiero wówczas, kiedy zagrożenie staje się realne. Firmy, które na co dzień nie posiadają oprogramowania zabezpieczającego ryzykują kradzieżą i szyfrowaniem danych oraz zainfekowaniem całego mechanizmu przedsiębiorstwa. Wszystko to przekłada się na niepotrzebny zastój w pracy, utratę wiarygodności wśród klientów i straty finansowe – a w dobie konkurencji żadna organizacja nie powinna sobie pozwolić na takie zaniedbanie. Oprócz odpowiedniego oprogramowania, przedsiębiorcy powinni zainwestować także w monitoring ruchu sieciowego, który umożliwia wcześniejszą reakcję na ewentualne zagrożenia. Optymalnym rozwiązaniem w celu zapewnienia firmie odpowiedniego zabezpieczenia, jest skorzystanie z zewnętrznego wsparcia IT. Przedsiębiorcy mogą outsourcować część usług, dotyczących np. wyłącznie helpdesku, nie muszą delegować wszystkich działań informatycznych poza organizację. Taka opcja daje możliwość redukcji kosztów i współpracy z doświadczonymi specjalistami. Pamiętajmy o tym, że zapewnienie pełnego bezpieczeństwa swojej firmie to stały proces wymagający odpowiednich kompetencji. Podjęcie systematycznych działań wpływa na ograniczenie ryzyka i jest dobrą inwestycją w przyszłość przedsiębiorstw.

REKLAMA

AntiFraud Hub
to nowoczesna platforma do zapobiegania wyłudzeniom.

Wspierane obszary biznesowe

- Compliance
- Fraudy webowe
- Fraudy wewnętrzne
- Fraudy w obszarze ubezpieczeń
- Monitorowanie aplikacji kredytowych i leasingowych
- Monitorowanie transakcji w czasie rzeczywistym
- Zarządzanie informacją o beneficjencie rzeczywistym
- Anonimowe zgłaszanie nadużyć i ich późniejsza obsługa (whistleblowing)



www.impaqgroup.com

IMPAQ
A Gfi Group Company
gfi

GAZETA FINANSOWA
14–27 lipca 2017 r.

BIZNES RAPORT

NAJLEPSZE ROZWIĄZANIA IT DLA FIRM I INSTYTUCJI FINANSOWYCH

Szanowni Państwo

Czy wyobrażacie sobie funkcjonowanie dzisiejszej bankowości bez możliwości dokonywania transakcji online? Albo ubezpieczyciela, u którego na stronie nie możemy zrobić kalkulacji np. OC czy AC? Chyba nie. Podobnie jak większość z nas nie wyobraża sobie funkcjonowania firmy bez wewnętrznego Internetu, bez możliwości bukowania urlopów bez konieczności udawania się do kadr czy przedstawiania zwolnień lekarskich za pomocą połączenia online. Wszyscy z tych dobrodziejstw korzystamy, mało kto zaś zastanawia się, skąd się one biorą. Postanowiliśmy więc przybliżyć Państwu tych, którzy dbają o to, by nam z instytucjami finansowymi współpracowało się wygodnie i by te instytucje funkcjonowały sprawnie. Sprawdźcie, może któreś oprogramowanie z naszego zestawienia okaże się interesujące z Waszego punktu widzenia?

Nazwa firmy	Nazwa produktu	Opis produktu/rozwiązania/usługi
Asseco Data Systems	LEO CMS – (Contract Management System)	Aplikacja dla działów operacyjnych (back office) firmy leasingowej, kompleksowo wspierająca obsługę kontraktów leasingowych; jest systematycznie poszerzana o moduły dodatkowe, ułatwiające firmom leasingowym realizację różnorodnych zadań biznesowych, niezależnie od ich profilu czy wielkości. LEO CMS (Contract Management System), LEO LG (General Ledger) oraz LEO CFM (Car Fleet Management) stanowią centrum proponowanych rozwiązań dla sektora leasingowego. Umożliwiają one klientom skuteczną realizację różnorodnych zadań z zakresu back office, a przede wszystkim obsługę umów leasingowych wraz z dodatkowymi produktami, jak np. wynajem krótkoterminowy/długoterminowy, dzierżawa, zarządzanie flotą samochodową, różnego rodzaju ubezpieczenia (AC/OC/NW/Assistance, GAP, Life), likwidacja szkód komunikacyjnych, przeglądy i naprawy serwisowe, samochody zastępcze, wymiana opon oraz karty paliwowe.
Bazy i Systemy Bankowe	proElix	ProELIX – scentralizowana platforma rozliczeniowa umożliwiająca obsługę i zarządzanie zleceniami we wszystkich walutach i kanałach rozliczeniowych.proELIX to dedykowany, elastyczny system wymiany danych pomiędzy systemami eksploatowanymi w banku, a zewnętrznymi systemami rozliczeniowymi.System zapewnia obsługę krajowych komunikatów nominowanych w PLN w ramach systemów Elixir i SORBNET2. Obejmuje również obsługę krajowych i transgranicznych płatności uznaniowych w EUR, w tym płatności SEPA, zgodnie z międzynarodowymi standardami rozliczeń Jednolitego Obszaru Płatności w Euro, w ramach systemu Euro Elixir. System umożliwia także przetwarzanie płatności w walutach innych niż EUR.System proELIX posiada budowę modułową. Każdy z modułów może funkcjonować jako samodzielna aplikacja bankowa lub współpracować z pozostałymi komponentami proELIX w ramach jednolitej platformy rozliczeniowej.Zastosowanie platformy proELIX umożliwia obniżenie kosztów obsługi i utrzymania systemów rozliczeniowych w banku oraz usprawnienie procesów rozliczeniowych podnosząc sprawność operacyjną i wzmacniając pozycję banku na rynku.
BrainSHARE IT	SaldeoSMART	SaldeoSMART to innowacyjna aplikacja online wspierająca nowoczesną księgowość. System odczytuje zeskanowane dokumenty papierowe lub wygenerowane elektronicznie faktury w PDF i pobiera z nich informacje, tj. numer faktury, dane kontrahenta, datę wystawienia, sprzedaży czy zapłaty oraz rejestr VAT. Pozwala to na wyeksportowanie faktur do pliku i jego import w programie księgowym, jakiego używa dana instytucja. SaldeoSMART korzysta z mechanizmów OCR (Optical Character Recognition), które służą do rozpoznawania znaków w plikach graficznych. Dzięki temu jest w stanie znaleźć i odczytać dane zawarte w skanie faktury, bez konieczności ich ręcznego przepisywania. Dzięki zastosowaniu zaawansowanych algorytmów proces przetwarzania dokumentu jest szybki i skuteczny. Aplikacja dostępna jest w dwóch modelach: online w modelu SaaS (aplikacja jest utrzymywana na serwerach firmy BrainSHARE IT) oraz lokalnej – instalowanej na serwerach należących do firmy.
Comarch	Comarch Corporate Banking	System dla bankowości, która wspiera klienta w 4 najważniejszych obszarach: zautomatyzowanej wymianie danych, ulepszonym zarządzaniu procesami biznesowymi, wielokanałowej dostępności do operacji bankowych oraz zapewnieniu najwyższego poziomu bezpieczeństwa przy wykorzystaniu wielu metod uwierzytelniania, takich jak karty mikroprocesorowe, hasła jednorazowe, tokeny mobilne, certyfikaty PKI, czy nawet biometria. Dzięki łatwej integracji z systemami ERP jest uniwersalnym narzędziem usprawniającym obsługę transakcji oraz pozwalającym na realne obniżenie ich kosztów. Platforma jest dostępna w kanałach: internetowym – jako system bankowości internetowej, mobilnym – jako narzędzie do zarządzania finansami dla managera w firmie oraz web service – jako rozwiązanie ułatwiające obsługę masowych transakcji płatniczych. Modułowość oraz szerokie możliwości konfiguracyjne sprawiają, że rozwiązanie spełnia oczekiwania nawet najbardziej wymagających banków.
Ideo	Logito – platforma elektronicznego obiegu dokumentów	–Dla pracowników nie mają znaczenia kartki papieru, ale informacje, które są na nich zawarte. – Dobrze zorganizowany workflow zapewnia zmniejszenie ilości dokumentów jakie krążą po firmie. Skraca czas ich przetworzenia i ułatwia dostęp do informacji archiwalnych. Podnosi także poziom bezpieczeństwa informacji. Istotnym elementem wdrożenia jest także obniżenie kosztów operacyjnych firmy. Do wielu instytucji trafia nawet kilka tysięcy dokumentów dziennie. Sprawne zarządzanie ich obiegiem, szybki dostęp do pism, czy monitoring terminów załatwienia spraw to jedne z ważniejszych zadań stawianych przed systemem elektronicznego obiegu dokumentów. System Elektronicznego Obiegu Dokumentów i Informacji LOGITO zapewnia standaryzację, usystematyzowanie i koordynację przepływu korespondencji w przedsiębiorstwie. Pozwoli także łatwiej zarządzać dystrybucją projektów, dokumentów oraz informacji z uwzględnieniem czynnika czasu.
IMPAQ	AntiFraud Hub	AntiFraud Hub to nowoczesna platforma do zapobiegania wyłudzeniom. System w trybie online'owym monitoruje napływające wnioski kredytowe i leasingowe, transakcje bankowe i komunikaty dotyczące obsługi ubezpieczeń. W każdym z tych przypadków dokonywana jest ocena wiarygodności podmiotów związanych z operacją. Do oceny transakcji wykorzystywane są dane z wniosków historycznych i ich metadane, dane będące w posiadaniu instytucji finansowej oraz ogólnokrajowe bazy danych. Integralną częścią systemu są Baza Incydentów, Rejestr Dokumentów wspierający obsługę korespondencji z organami ścigania oraz moduł zarządzania alertami, sprawami i zadaniami. Dzięki modularnej budowie system pozwala na wykorzystanie tej bazy wiedzy także do zapobiegania oszustwom w kanale internetowym, poprzez analizę komunikacji pomiędzy urządzeniem klienta a aplikacją chronioną, budowanie profili zachowań klientów i ich urządzeń. Ta część systemu potrafi także rozpoznać niektóre rodzaje infekcji (malware) w urządzeniu klienta, oraz wskazać transakcje zlecane z użyciem mechanizmów anonymizacji. System działa w infrastrukturze klienta, ale niedługo dostępny będzie jako usługa (SaaS).
Risco Software	Risco Zarządzanie Gotówką Banku	System do pełnej automatyzacji i obsługi zarządzania obrotem gotówką w banku. Zintegrowany system informatyczny do zarządzania gotówką. Autorski produkt Risco Software. Umożliwia centralne zarządzanie gotówką zwalniając tym samym roboczogodziny dedykowanych pracowników banku. Oferuje pełną obsługę procesów zarządzania gotówką. Głównym celem stworzenia systemu Risco Zarządzanie Gotówką Banku jest poprawa procesów zarządzania gotówką w banku poprzez ich automatyzację, której rezultatem ma być zmniejszenie kosztów utrzymania gotówki. System generuje oszczędność czasu związaną z automatyzacją części prac dotychczas realizowanych ręcznie (w tym m.in. procesu zamawiania, rozliczeń księgowych, generowania wydruków itd.). Dotychczasowe kanały zamawiania zasileń i odprowadzeń gotówki zostają zastąpione. System jest w pełni przygotowany do integracji z innymi systemami banku, ogranicza ryzyko operacyjne i zapewnia odpowiedni poziom bezpieczeństwa.
Sente	Sente S4	Sente S4 to kompleksowa platforma informatyczna do wspierania firm w ich codziennym funkcjonowaniu. Nasz system już od 2000 r. usprawnia zarządzanie w średnich i dużych przedsiębiorstwach. Stale rozwijamy nasze oprogramowanie, aby szło w parze ze zmianami na rynku i potrzebami naszych klientów. Sente S4 to nie zwykły system ERP, bo oprócz rozwiązań klasy ERP swoją funkcjonalnością obejmuje CRM, DMS, WMS, MES, WORKFLOW, umożliwiając firmie obsługę wszystkich wewnętrznych procesów operacyjnych w jednym, zintegrowanym środowisku. Główny cel, który Sente S4 pomaga osiągnąć przedsiębiorcom, to rozwój firmy dzięki zwiększeniu efektywności jej codziennej pracy. Przed biznesem stoi coraz więcej wyzwań, a Sente S4 ma pomóc im sprostać i pozwolić zdobyć przewagę konkurencyjną. Nasza aplikacja pozwala zarządzać zasobami firmy, ale inaczej niż zwykłe systemy ERP, koncentrując się na przebiegu procesów i efektywnym realizowaniu zadań w organizacji.
Sygnity	Sygnity IntelliBanking	Sygnity IntelliBanking jest nowoczesną platformą inteligentnych kanałów elektronicznych realizowaną w koncepcji omnichannel pozwalającą dostarczyć spójny interfejs bankowości internetowej i mobilnej. Jednocześnie Sygnity Intellibanking stanowi aktywną biznesowo platformę, której zastosowanie przekłada się na liczne benefity banków i ich klientów. Rozwiązanie odpowiada na potrzeby banków i wymagania stawiane przez rynek globalny oraz, co najważniejsze, klientów poszukujących spersonalizowanych usług bankowych a nie samych banków. System umożliwia inteligentne targetowanie, w czasie rzeczywistym, pozwalające na przygotowanie dopasowanej i personalizowanej oferty w oparciu o analizę profilu klienta, w tym: jego zachowań społecznych i biznesowych, interakcji, realizowanych transakcji i posiadanych produktów, czyli tzw. Customer Intelligence. Za pomocą wbudowanych narzędzi analitycznych, system dostarcza bankowi informacji o preferencjach klienta i tego w jaki sposób oraz gdzie korzysta z usług bankowych, tym samym wspiera użytkownika na każdym etapie codziennego korzystania z usług bankowych oraz angażuje go w większą interakcję z bankiem. Platforma Sygnity IntelliBanking dostarcza takiej kombinacji produktów i procesów, które umożliwiają klientowi optymalne korzystanie z usług bankowych.
TUKAN IT	GREENmod	GREENmod jest systemem przeznaczonym do klasyfikacji dokumentów. To jedyne polskie rozwiązanie umożliwiające zaangażowanie użytkowników końcowych w proces klasyfikacji informacji. GREENmod, autorskie oprogramowanie firmy Tukan IT, uzupełnia automatyczne mechanizmy klasyfikacji (systemy takie jak DLP, RMS) o nieocenioną wiedzę użytkownika dotyczącą poufności tworzonych przez niego treści. System GREENmod jest rozwiązaniem, które umożliwi dokonanie odpowiedniej weryfikacji informacji, ponieważ wymusi na użytkowniku – czyli na twórcy informacji – klasyfikację wytwarzanych danych. GREENmod nie pozwoli na zapisanie, czy też wysłanie informacji bez odpowiedniej kategoryzacji. Taką klasyfikację w postaci metadanych można wykorzystać w politykach DLP w powiązaniu z innymi funkcjami, takimi jak, szczegółowa analiza zawartości poprzez wyszukiwanie za pomocą słów kluczowych, słowników, wyrażeń regularnych, zdefiniowanych szablonów takich jak np. weryfikacja sumy kontrolnej z numerów kart kredytowych itp. Stosowanie GREENmod znacząco wpływa na podnoszenie świadomość pracowników w zakresie bezpieczeństwa informacji firmowych.

Hakerzy celują w Polskę

Wojciech **Głażewski**

country manager Check Point Software Technologies

Polska staje się celem ataków hakerskich. Ulokowaliśmy się na 6. miejscu w Europie wśród krajów z największą liczbą ataków, z indeksem zagrożenia na poziomie 34,4 pkt. Tym samym przesunęliśmy się o 12 miejsc i jesteśmy krajem, w którym zagrożenie wzrasta. Poza czołową trójką gorszymi wskaźnikami charakteryzują się tylko Rosja i Rumunia (odpowiednio 38,8 i 35,9) – pokazał raport dotyczący cyberbezpieczeństwa.

Codziennie doświadczamy ponad 26 tys. ataków na świecie. Jak wynika z badań PwC w Polsce 96 proc. firm doświadczyło co najmniej 50 ataków w ciągu roku, jednocześnie wzrosły koszty wynikające z cyberataków. Średni koszt jednorazowego ataku na polską firmę sięga 1,5 mln złotych. Firmy na pewno powinny coraz bardziej myśleć o bezpieczeństwie i to w ujęciu całościowym, jako kompleksowej polityki bezpieczeństwa. Czy zagrożenie będzie rosło? Na pewno takich ataków będzie więcej, ponieważ one są coraz prostsze do przeprowadzenia.W Internecie są dostępne narzędzia, które pozwalają nawet osobom niespecjalnie wyedukowanym zlecić taki atak. W skali europejskiej najbardziej zagrożonymi krajami są: Macedonia (69,6), Gruzja (62,6) i Albania (53,3). Na przeciwnym biegunie znalazły się Mołdawia (20,4), Islandia (20,7) oraz Luksemburg (21,9), które w maju odnotowały najmniejszą liczbę incydentów bezpieczeństwa wśród 42 sklasyfikowanych państw Europy.

BIZNES RAPORT
GAZETA FINANSOWA
14–27 lipca 2017 r.

Technika – Procedury – Ludzie System do klasyfikacji dokumentów

W 2016 i 2017 roku branża finansowa, medyczna i motoryzacyjna znalazły się w centrum zainteresowania cyberprzestępców na świecie. Doszło do spektakularnych wycieków danych, a bezpieczeństwo danych stało się jednym z głównych tematów.

Mimo to, nadal wielu menadżerów uważa, że bezpieczeństwo danych to domena obszaru IT, a nie krytyczny czynnik funkcjonowania przedsiębiorstwa. Kluczem do skutecznej ochrony przed cyberatakami czy wyciekiem danych, jest budowanie świadomości wśród pracowników i klientów firm. Dojrzałe instytucje wyciągają z tego wnioski i dostrzegają, że cyberbezpieczeństwo to nie tylko sprzęt i systemy bezpieczeństwa, ale także ludzie.

Podnieść na wyższy poziom

Według wielu opracowań (m.in. Komisji Europejskiej i Ministerstwa Cyfryzacji), bezpieczeństwo w cyberprzestrzeni określają trzy podstawowe obszary: Technika – Procedury – Ludzie. Analizy aktualnego stanu w większości przypadków wskazują, że o ile obszar techniczny jest zabezpieczony w stopniu co najmniej zadowalającym i należy jedynie dbać o jego dalszy rozwój, to w przypadku pozostałych dwóch obszarów – Procedury i Ludzie – konieczne jest jak najszybsze zainicjowanie działań rozwojowych. Dlatego też główny nacisk kładzie się na sferę organizacyjną systemu bezpieczeństwa w cyberprzestrzeni. Kluczem do skutecznej ochrony przed cyberatakami jest budowanie świadomości i edukacja użytkowników będących najsłabszym ogniwem cyberbezpieczeństwa polskich przedsiębiorstw.

Ważne zadanie

Odpowiedzialność za cyberbezpieczeństwo powinna spoczywać na każdej osobie zatrudnionej w przedsiębiorstwie, a nie tylko na barkach zarządu. Należy więc radykalnie zmienić sposób rozmawiania o bezpieczeństwie i zaangażować w nie również pracowników. Połowa dużych firm w Polsce planuje w najbliższych dwóch latach zwiększyć inwestycje w obszarze bezpieczeństwa informatycznego. To efekt rosnącego zagrożenia cyberprzestępstwami. Uświadamianie pracowników to najtrudniejsze, ale jednocześnie najważniejsze zadanie dla osób odpowiedzialnych za bezpieczeństwo w firmie. Kluczem do tego jest ciągła edukacja i komunikacja, a nie jednorazowe akcje – powiedziała Katarzyna Budna-Grzęda, Prezes TUKAN IT.

W idealnym systemie każdy pracownik powinien mieć poczucie, że uczestniczy w procesach odpowiadających za bezpieczeństwo cybernetyczne firmy. Im bardziej pracownicy są świadomi, tym skuteczniejszy będzie ten „ludzki firewall". Poprzez edukację można wyeliminować nawet do 99 procent wszystkich zdarzeń związanych z bezpieczeństwem informatycznym.

Sprawdzone rozwiązania

W realizacji procesu podnoszenia świadomości dotyczącej wagi przetwarzanych informacji warto wykorzystać systemy, dzięki którym użytkownik nie tylko uczy się, ale też staje się istotnym elementem procesu bezpieczeństwa.

Jednym z takich narzędzi jest GREENmod firmy TUKAN IT. Rozwiązanie to przeznaczone jest do klasyfikacji informacji wytwarzanych przez użytkownika końcowego, czyli pracownika. Wprowadza ono możliwość uzupełnienia mechanizmów automatycznie kategoryzujących dokumenty oraz pocztę elektroniczną o nieocenioną w takich przypadkach wiedzę użytkownika, dotyczącą poufności tworzonych przez niego treści. Rozwiązanie to integruje się z aplikacjami Microsoft Office oraz systemem operacyjnym Microsoft Windows, wymuszając konieczność sklasyfikowania tworzonego dokumentu przed jego zapisaniem. Analogicznie, GREENmod uniemożliwi wysłanie wiadomości pocztowej, jeżeli nie zostanie ona sklasyfikowana. Użytkownik może również nadawać odpowiednie poziomy klasyfikacji wielu innym dokumentom spoza pakietu Office, do których ma dostęp.

Znaczniki nadawane w procesie klasyfikacji są łatwo rozpoznawane przez różnego rodzaju rozwiązania analizujące treść i właściwości dokumentów (systemy DLP, RMS, rozwiązania mail i web proxy, itp.). Na ich podstawie możliwe jest wobec tego skuteczne egzekwowanie przyjętej w organizacji polityki bezpieczeństwa i świadome podejmowanie decyzji dotyczących sposobu obsługi, przetwarzania oraz ochrony danych treści. Świadomość tego, z jakimi informacjami mamy do czynienia, korzystnie wpływa także na koszty ponoszone na ich zabezpieczenie.

Podnoszenie świadomości

Wykorzystanie rozwiązania Tukan IT GREENmod w organizacji znacząco wpływa na podnoszenie świadomości pracowników dotyczącej zagadnień bezpieczeństwa oraz ważności przetwarzanych przez nich informacji. W efekcie spada także liczba incydentów związanych z wyciekiem informacji spowodowanych czynnościami wykonywanymi bez zastanowienia lub ze względu na brak wiedzy o skutkach udostępnienia chronionych treści osobom nieupoważnionym. Pracownicy, którzy są zaangażowani w proces zapewniania bezpieczeństwa, stają się bardziej odpowiedzialni za informacje, które tworzą.

Adekwatnie do wymagań

Konieczność stosowania opisywanych rozwiązań wynika także z zewnętrznych regulacji, takich jak GDPR, w których duży nacisk kładzie się na ochronę danych przetwarzanych przez firmy w ich systemach teleinformatycznych, z uwzględnieniem ryzyka nieuprawnionego dostępu do informacji. Jednym z rozwiązań umożliwiających realizację podejścia opartego o ryzyko jest właśnie system wspomagający klasyfikowanie dokumentów oraz poczty elektronicznej jak GREENmod. – tłumaczy – Katarzyna Budna-Grzęda, Prezes TUKAN IT.

Systemy klasy DLP (Data Loss Prevention), posiadające zaawansowane mechanizmy automatycznej klasyfikacji treści, są niestety często „nieczułe" na specyficzne rodzaje zawartości, niepoddające się algorytmom klasyfikacji. Systemy wspomagające klasyfikację, wprowadzają możliwość uzupełnienia mechanizmów automatycznego klasyfikowania dokumentów oraz poczty elektronicznej o nieocenioną, w takich przypadkach, wiedzę użytkownika dotyczącą poufności tworzonych przez niego treści.

Dlaczego warto stosować systemy do klasyfikacji dokumentów?

Podnoszą świadomość bezpieczeństwa. Wykorzystanie takiego rozwiązania, bardzo pozytywnie wpływa na podnoszenie świadomości pracowników organizacji, dotyczącej zagadnień bezpieczeństwa oraz ważności przetwarzanych przez nich informacji.

Przenoszą odpowiedzialność za ochronę danych na twórców dokumentów. Działy Bezpieczeństwa funkcjonujące w organizacjach, często nie potrafią wskazać metod klasyfikowania informacji, które możliwe byłyby do zaimplementowania w systemach klasy DLP. Twórca dokumentu jest najlepszym źródłem informacji o poprawnej klasyfikacji wyników jego pracy. Klasyfikacja nadana przez użytkownika stanowić będzie pierwszą linię ochrony, uzupełniającą automatyczne metody klasyfikacji zapewniane rozwiązaniami klasy DLP.

Łatwo integrują się z systemami klasy DLP. System oznaczania dokumentów (metadane dodawane do plików i wiadomości pocztowych) może być wykorzystywany do automatyzacji procesów ochrony, między innymi takich jak:

- monitorowanie
- blokowanie transferu danych
- zapobieganie drukowaniu
- alarmowanie o naruszeniach bezpieczeństwa
- poddawanie kwarantannie
- szyfrowanie danych
- archiwizowanie

Tukan IT GREENmod:

- Angażuje użytkowników w proces klasyfikowania informacji
- Umożliwia dostosowanie struktury klasyfikacji do własnych potrzeb
- Integruje się z systemami chroniącymi i przetwarzającymi informacje
- Posiada centralne zarządzanie i raportowanie
- Pomaga ustalić odpowiedzialność i właściciela informacji
- Wspomaga procedury audytowe
- Obniża koszty zabezpieczania informacji

GREENmod
SYSTEM DO KLASYFIKACJI INFORMACJI
TUKAN IT
tukanit.pl

TEKST PROMOCYJNY