

Outsourcing IT Bezpieczeństwo staje się coraz ważniejsze

Usługodawcy dbają

Podobno firmy outsourcingowe są w stanie zaproponować klientowi poziom bezpieczeństwa usług IT wyższy niż ten, który klient może zapewnić we własnym zakresie.

Pracownicy firm świadczących usługi outsourcingu doskonale zdają sobie sprawę, że spokój klientów o bezpieczeństwo ich danych jest wiele wart. Dlatego podejmują działania mające na celu radzenie sobie z tymi obawami.

— Najlepszym zabezpieczeniem jest brak dostępu do danych istot-

nych dla firmy przez pracowników usługodawcy. Czyli np. sieć LAN jest zarządzana przez firmę zewnętrzną, która jednak nie ma dostępu do danych zawartych na serwerach. Ponadto klient nadal zachowuje kontrolę działań — czyli to jego pracownicy muszą nadzorować pracę firmy dbającej o dane — przekonuje Michał Grzech z NextiraOne Polska.

Odpowiedni standard bezpieczeństwa i transmisji danych ma być osiągany przez zwielokrotnienie zabezpieczeń fizycznych i przez działania techniczne. Zabezpieczenia takie mają skutecznie eliminować podstawowe zagrożenia utraty danych, czyli: ataki włamy-

waczy komputerowych, wirusy, próby nieautoryzowanego dostępu lub kradzieży informacji przez osoby zewnętrzne.

— Najważniejsza jest długa praktyka zapewnienia bezpieczeństwa klienta, wynikająca ze świadomości, że usługi muszą być pewne pod względem ochrony danych i ciągłości pracy systemu. Jest to stały, trwały element kultury korporacyjnej, który można stworzyć tylko przez długotrwałe stosowanie. W przypadku firm, które niedawno weszły na rynek, nie jest to takie oczywiste, gdyż decyduje tu nie tylko zainstalowana infrastruktura, lecz także personel, który musi nabyć wspomniane elemen-

ty kultury usług outsourcingu IT — twierdzi Janusz Dorożyński, główny technolog, który odpowiada w ZETO Poznań za kwestie związane z bezpieczeństwem.

Aktywnie

Według Arnolda Nowaka, członka zarządu firmy itelligence, profesjonalna firma outsourcingowa traktuje bezpieczeństwo trójaspektowo — musi zapewnić systemom swoich klientów bezpieczeństwo techniczne, technologiczne i psychologiczne.

— Na straży bezpieczeństwa technicznego stoją data center — serwerownie zabezpieczone zarówno przed dostępem osób niepowo-

lanych, jak i przed zdarzeniami losowymi. Bezpieczeństwo technologiczne zapewnia najnowszy sprzęt i oprogramowanie oraz odpowiednie procedury. Co do bezpieczeństwa psychologicznego, specjaliści mają przewagę nad własnymi administratorami klienta — nie znają biznesu klienta, więc nie wiedzą, które informacje są dla niego strategiczne — twierdzi Arnold Nowak.

Ale i firma chcąc zlecić opiekę nad swoją infrastrukturą nie może pozostać bierna.

— Teoretycznie wiadomo, jakie stosuje się obecnie technologie i rozwiązania zapewniające ciągłe i bezpieczne świadczenie usług. Weryfikacja rozwiązania proponowanego przez dostawcę to sprawdzenie, w jaki sposób dzisiaj świadczy usługi outsourcingu i na ile jego klienci są zadowoleni. Dodatkowo poziom bezpieczeństwa zależy od poziomu inwestycji, czyli jaką kwotę zechce zapłacić usługobiorca, aby zabezpieczyć prowadzony biznes — twierdzi Anna Sieńko z IBM Polska.

U specjalisty

Przedstawiciele firm potencjalnie zainteresowanych współpracą z firmą outsourcingową zastanawiają się, czy i w jaki sposób zewnętrzny usługodawca może zagwarantować



PO IMIENIU Ważne jest określenie pomiędzy definicji i uniknięcie dzięki temu niebezpieczeństwa pretacji ocenianych zachowań — przekonuje J. Wdrożeń Incenti.

O spokojój klientów

Bezpieczeństwo niejedno ma imię

wyższy poziom bezpieczeństwa danych i ich transmisji niż wewnętrzny dział IT przedsiębiorstwa.

— Moim zdaniem, korzystanie z usług outsourcingu IT jest rozwiązaniem zdecydowanie bezpieczniejszym dla firmy niż własny dział informatyki. Firma outsourcingowa jest w stanie zaproponować swojemu klientowi znacznie wyższy poziom bezpieczeństwa usług IT niż ten, który klient może sobie zapewnić we własnym zakresie. Dostawca usług w sposób oczywisty jest zainteresowany jak najwyższym poziomem bezpieczeństwa swojego produktu, gdyż stanowi to o jego renomie — przekonuje Janusz Dorożyński.

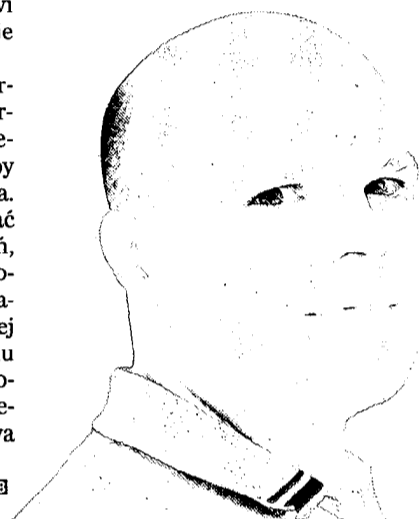
— Po pierwsze, firmy outsourcingowe mogą zaproponować bardziej rozbudowane zabezpieczenia, na których zakup nie mogłaby sobie pozwolić przeciętna firma. Oprócz tego mogą zaproponować dodatkowe usługi zabezpieczeń, takie jak np. ochrona antywirusowa, które w przeciwieństwie do zakupu, takich rozwiązań do własnej sieci nie kosztują kilkudziesięciu tysięcy dolarów, tylko kilkaset złotych miesięcznie — dodaje Grzegorz Flak z działu bezpieczeństwa Comarchu.

Marcin Złoch ☒

m.zloch@pb.pl ☎ (22) 334-20-61

Najczęstsze obawy klientów to: utrata kontroli nad rozwojem IT, wzrost kosztów lub brak elastyczności we wprowadzaniu zmian.

Można być niemal pewnym, że podczas dyskusji na temat outsourcingu usłyszymy głosy o „bezpieczeństwie”. Ale co należy ro-



zumieć pod pojęciem „bezpieczeństwa” w kontraktach outsourcingowych? Anna Sieńko z IBM Polska wylicza, że można wyróżnić elementy bezpieczeństwa fizycznego dostępu, ciągłości świadczenia usług lub bezpieczeństwa danych.

— W kontraktach outsourcingowych bezpieczeństwo pojawia się w podwójnym znaczeniu. Z jednej strony klienci pytają się o bezpieczeństwo operacyjne, a więc parametry SLA, wiarygodność firmy i jej pracowników. Drugim aspektem jest bezpieczeństwo informacyjne, czyli w jaki sposób firma outsourcingowa dba o dostępność, poufność i integralność danych — mówi Grzegorz Flak z działu bezpieczeństwa Comarchu.

Janusz Dorożyński, główny technolog, który odpowiada w ZETO Poznań za kwestie związane z bezpieczeństwem, potwier-

dza, że klienci firm outsourcingowych bezpieczeństwo postrzegają zarówno jako fizyczną ochronę swoich danych, jak i ciągłość oraz wydajność gwarantowane umową SLA.

— Najistotniejszym aspektem bezpieczeństwa, które powinien gwarantować kontrakt outsourcingowy jest bezpieczeństwo utrzymania i rozwoju biznesu klienta. Oznacza to konieczność wprowadzenia takich zapisów do kontraktu, które umożliwią elastyczność usług i ich dopasowanie do przyszłych zmian w biznesie — twierdzi Anna Sieńko.

Strachliwi

Według przedstawicieli firm oferujących usługi, już sam fakt współpracy może mieć wpływ na wzrost bezpieczeństwa danych.

— Kontrakt oznacza dla klienta przewidywalność kosztów ponoszonych na IT i gwarancje dzia-

łania systemów — przekonuje Jacek Konczewski, dyrektor działu projektowania i wdrożeń Incenti.

Pomimo zapewnień, klienci firm IT nie ukrywają obaw o bezpieczeństwo danych.

— Najczęstsze obawy to utrata kontroli nad rozwojem IT, wzrost kosztów czy brak elastyczności we wprowadzaniu zmian — informuje Anna Sieńko.

Na wypadek

Awarie się zdarzają, także w przypadku umów outsourcingowych.

— Wiadomo, że nie ma systemów w 100 proc. odpornych na awarie i ataki. Zaletą usług outsourcingowych jest to, że data center w takiej firmie wyposażone jest w zabezpieczenia techniczne, na jakie klient takich usług się nie zdecydował. Mam tu na myśli kaskadę zapór ogniowych, systemy wykrywania i przeciwdziałania włamaniom, wielopoziomowe zabezpieczenia antywirusowe, zdublowanie sieci czy zasilacze awaryjne — twierdzi Grzegorz Flak.

Marcin Złoch ☒

m.zloch@pb.pl ☎ (22) 334-20-61



stronami kontraktu outsourcingowego wspólnych stron pojawiają się w przyszłości różnych inter-

— Jacek Konczewski, dyrektor działu projektowania i

— fot. GK

ZAPORY Krytyczne aplikacje każdego naszego klienta chronione są przez podwójną kaskadę systemów zaporowych. Rozwiązania takie stosują na ogół tylko najbardziej wymagające firmy, takie jak banki czy telekomunikacja — twierdzi Grzegorz Flak z działu bezpieczeństwa Comarchu. fot. ARC