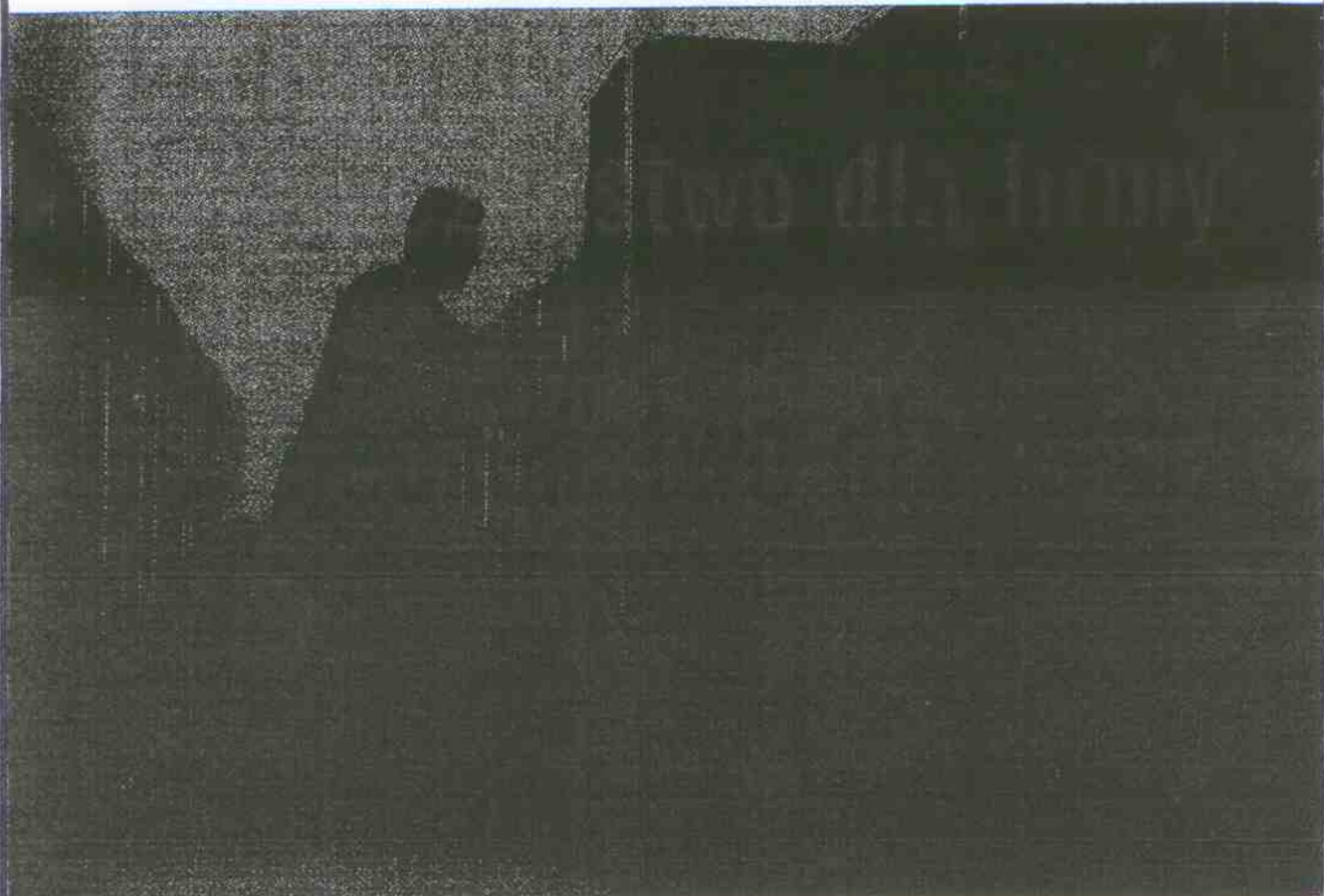


Bezpieczeństwo dla firmy



Bezpieczeństwo oferowanych w outsourcingu usług IT jest dla outsourcera podstawowym warunkiem przetrwania na rynku. Wartość danych dla firmy jest bezcenna.

Systemy zapewniające ich bezwarunkowe bezpieczeństwo są jednak zwykle zbyt drogie, aby można je było wdrażać indywidualnie. Nikt nie kupuje mleczarni tylko po to, by móc co rano pić świeże mleko. Dla outsourcera bezpieczeństwo jest produktem, a produkt ten musi być atrakcyjny, wysokiej jakości i z gwarancją. To wyspecjalizowana firma zewnętrzna stale inwestuje w rozwój swojej specjalizacji, korzysta z doświadczenia i jest przygotowana na najbardziej nieoczekiwane zagrożenia. Dlatego może ona zaoferować nieporównanie wyższy standard bezpieczeństwa niż ten, który byłby w stanie samodzielnie zbudować jej klient. Często zdarza się, że proponowane przez outsourcera rozwiązania zawierają elementy, których istnienia klient, ze względu na bardzo

szybko rozwijającą się technologię IT, nie jest nawet świadomy.

Standardy

Na standard bezpieczeństwa składają się zabezpieczenia techniczne i technologiczne. Centrum Systemów Informatycznych w Tarnowie Podgórnym pod Poznaniem mieści się w budynku, który został w tym celu zaprojektowany i wykonany. Bezpieczeństwo techniczne zapewniają specjalne procedury, obejmujące podział: na strefy, monitorowanie, alarmy antywłamaniowe i pożarowe, elektroniczną kontrolę dostępu, infrastrukturę, na którą składają się własne łącza światłowodowe do różnych operatorów telekomunikacyjnych, łącza zapaso-

we w różnych technologiach, dwa niezależne agregaty prądowców, odpowiednie, redundantne UPS-y i niezawodna klimatyzacja. Bezpieczeństwo technologiczne zapewnia najnowszy sprzęt, oprogramowanie oraz najnowsze rozwiązania w dziedzinie zarządzania informacją. Kopie bezpieczeństwa wykonywane są na niezawodnym sprzęcie, a nośniki są przechowywane w ogniotrwałym sejfie lub przewożone do skrytek bankowych.

Antidotum na strach

Każda firma narażona jest na wyciek wewnętrznych informacji i danych. Nielojalni pracownicy zdarzają się wszędzie. Pracownicy outsourcingera podlegają specjalnym procedurom rekrutacji, weryfikacji i szkolenia, jakie trwają przez cały okres zatrudnienia, a ich praca jest nadzorowana przez specjalnie do tego wyszkolony, świadomy potrzeby przestrzegania procedur personel. Pozwala to ściśle kontrolować ryzyko ewentualnego wycieku informacji i podjąć odpowiednie działania, zanim taka sytuacja mogłaby mieć miejsce. Mimo tak restrykcyjnego podejścia do tajemnicy powierzonej informacji – może zdarzyć się ktoś, kto jednak dopuści się nadużycia. Wówczas outsourcinger jest zobowiązany prawnie i finansowo do wypłaty odszkodowania, a dotrzymanie warunków, odszkodowań i kar reguluje zawarta umowa. To samo dotyczy innych parametrów systemu, równie ważnych jak poufność informacji, np.: dostępność, czas odpowiedzi, czas reakcji w przypadku stwierdzonych nieprawidłowości itp.

Umowa i jej zabezpieczenie

W kontrakcie outsourcingowym nie można przewidzieć każdej sytuacji. Dziedzina IT jest skomplikowana, a technologia szybko się zmienia. Dlatego tak ważne jest precyzyjne sformułowanie umowy. Umowa typu SLA (Service Level Agreement) określa nie tylko obowiązki i odpowiedzialność dostawcy usług outsourcingowych, ale także zobowiązuje outsourcingera do rzetelnego ich wykonywania. Zagrożeniem jest niedotrzymanie gwarantowanych parametrów wynikających z zapisów umowy SLA. Dlatego podczas realizacji umów outsourcingowych działa precyzyjny system monitoringu oraz system rejestracji zgłoszeń (błędy, awarie itp.) zdolny do mierzenia odpowiednich parametrów wykonania usługi. Wiarygodność outsourcingera w zakresie dotrzymania parametrów umowy podnoszą wdrożone przez niego syste-

my jakości, np. normy jakości ISO 9001:2000 czy też BS 7799-2.

Obustronna ostrożność

Dostawcy usług outsourcingowych przez całe lata dążyli do rozwiania obaw klientów związanych z bezpieczeństwem. Profesjonalny dostawca czyni to nadal w bezpośrednich kontaktach z każdym potencjalnym klientem, a z tymi, którzy zdecydowali się na taką formę usług, negocjuje punkt po punkcie warunki umowy SLA, rozpatrując i wyjaśniając wszelkie wątpliwości. Metody weryfikacji potencjalnego usługodawcy są takie same jak w innych obszarach IT – warto obejrzeć jego centrum przetwarzania danych i zasięgnąć opinii klientów referencyjnych. Pewną wskazówką mogą być certyfikaty (np. status SAP Global Hosting Partner).

Podstawą prawidłowo spisanej umowy jest dokładna definicja zakresu usług, która powinna obejmować ich gwarantowany poziom (czas odpowiedzi, dostępność, czas reakcji itp.) oraz zasady współpracy stron. Jest szczególnie ważne, żeby ustalić wzajemną odpowiedzialność, a także precyzyjny sposób komunikacji i raportowania podczas trwania umowy. Niezbędny jest także przejrzysty cennik usług. Do niezwykle ważnych elementów umowy należą gwarancje outsourcingera – jeśli będą niespełnione, klient ma prawo domagać się kar umownych. Umowa musi także nie tylko przewidywać sytuacje nadzwyczajne, spowodowane np. kataklizmami, ale i uwzględniać procedury ratunkowe. Ważne jest też zdefiniowanie warunków wypowiedzenia i zasad zakończenia współpracy.

Podczas negocjacji trzeba pamiętać, że – chociaż nie uda się przewidzieć każdej sytuacji konfliktowej – umowa powinna stanowić solidną podstawę do rozstrzygnięcia większości spraw spornych.

Wydaje się, że model outsourcingu wzbudza obecnie mniej obaw, bo klienci przekonali się, iż umowa outsourcingowa jest umową gwarantującą określony poziom usług, czego nigdy nie będą w stanie wyegzekwować od własnego działu IT.

Wojciech Darłowski
dyrektor Centrum
Systemów Informatycznych
Intelligence Sp. z o.o.