Warszawa, 25.03.2015 r.

Komunikat prasowy

Wyzwania w zakresie ochrony danych w chmurze - czy zrobiłeś wszystko, żeby chronić dane swojej firmy?

Rozwiązania chmurowe z każdym dniem zyskują coraz większą popularność. Są wykorzystywane przez firmy, żeby zwiększyć efektywność zarządzania kluczowymi informacjami w przedsiębiorstwie, ułatwić dzielenie się informacjami, czy przyspieszyć realizowane procesy biznesowe. Wraz z ich popularnością, jak nigdy wcześniej kluczowego znaczenia nabiera tematyka bezpieczeństwa danych firmowych utrzymywanych w popularnie zwanej chmurze.

Luki bezpieczeństwa, takie jak ubiegłoroczne Heartbleed, czy Shellshock, ataki hackerskie, które nie oszczędzają nawet największych (Sony Pictures i pozyskanie ponad 100 terabajtów danych (30 tysięcy plików), Adobe i wyciek danych 33 mln klientów firmy, czy wyciek kluczowych informacji jak to było w przypadku Dropboxa) to tylko wybrane przykłady, które pokazują, że w temacie bezpieczeństwa IT zdecydowanie ma nad czym się pochylać. Ale nie tylko IT powinno stać na baczności. Na równi z ujawnionymi lukami bezpieczeństwa, sen z powiek organizacji spędzają bowiem miękkie aspekty bezpieczeństwa, takie jak brak odpowiednich procedur w firmie, nieodpowiednio przeszkolony personel, czy po prostu ryzyko błędu ludzkiego. Zagrożeniem mogą być także aktualne trendy, takie jak BYOD, które rodzą kolejne wyzwania, zarówno dla IT, jak i dla biznesu.

O czym zatem należy pamiętać decydując się na wybór rozwiązań chmurowych?

Przede wszystkim pamiętajmy, że bezpieczeństwo danych firmowych w sieci to nie tylko kwestia zabezpieczeń fizycznych, jakie stosuje dostawca danego rozwiązania. Są to oczywiście kwestie ogromnie ważne, ale nie jedyne jeśli chcemy kompleksowo zadbać o bezpieczeństwo. Trzeba zwrócić uwagę także na takie aspekty jak ludzie, procedury stosowane w organizacji, czy rozwiązania prawne. Te ostatnie nabrały znaczenia szczególnie w obliczu szeroko dyskutowanego w zeszłym roku tematu dostępu władz amerykańskich do danych klientów tamtejszych firm. Ich przypieczętowaniem był wyrok amerykańskiego Sądu z 31 lipca, na mocy którego Microsoft ma obowiązek przekazywać dane klientów (np. przechowywanych w poczcie elektronicznej) amerykańskim władzom nawet wtedy, gdy są one składowane na serwerach znajdujących się w Dublinie. Wskazuje się, iż również inne firmy amerykańskie, tj. Google, Yahoo, czy Apple zobowiązane są do przekazywania dostępu do danych użytkowników.

Regulacje prawne

Skoro o aspektach prawnych mowa. Weźmy za przykład niezwykle wrażliwe na poufność i bezpieczeństwo danych procesy transakcyjne, takie jak debiuty giełdowe, czy fuzje i przejęcia. W ich realizacji od dawna wykorzystywane są chmurowe rozwiązania do zarządzania dokumentami, tj. **Virtual Data Room**. Dla spółek polskich (szczególnie tych publicznych) znaczenie ma nie tylko to, gdzie dostawca takiego systemu kolokuje swoje

serwery, ale także to, na jakiej podstawie prawnej działa. Kluczowe jest, aby proces był prowadzony zgodnie z obowiązkiem informacyjnym, jakiemu podlegają spółki, a w przypadku ewentualnych sporów z podmiotami zewnętrznymi, aby były one rozwiązywane na gruncie polskiego ustawodawstwa.

Jak pokazuje wspomniany wyrok, lokalizacja serwerów i miejsce rejestracji firmy także bezpośrednio determinują poziom bezpieczeństwa i integralności danych. Największy poziom ochrony gwarantują dostawcy europejscy, którzy posiadają swoje serwerownie na terenie Unii Europejskiej, ponieważ chroni je **Dyrektywa UE w sprawie ochrony danych osobowych (Data Protection Directive)**, prawdopodobnie najbardziej rygorystyczna polityka w tym zakresie na świecie. W przypadku serwerów utrzymywanych poza obszarem UE, poziom zapewnienia poufności dla wrażliwych danych jest zdecydowanie mniejszy. A już najmniejszy w przypadku dostawców amerykańskich, nawet tych, którzy przenieśli swoje serwery do Europy.

Procedury i ludzie u dostawcy rozwiązania

Wiele firm myśląc o bezpieczeństwie danych, często pomija ryzyko związane ze zwykłym błędem ludzkim. Zaniedbania pracowników w tym zakresie są często nieświadome, jednak ich konsekwencje mogą być naprawdę poważne. Spójrzmy na takie działania jak pozostawienie laptopa bez nadzoru, brak stosowania bezpiecznych haseł, używanie nieszyfrowanych nośników typu pendrive, czy zabieranie danych firmowych na pendrive do domu i praca w niezabezpieczonej sieci. W organizacjach z odpowiednimi procedurami bezpieczeństwa i przeszkolonym personelem takie zaniedbania nie są możliwe.

Dlatego decydując się na rozwiązania chmurowe upewnijmy się, że dostawca ma wdrożone odpowiednie procedury i dobrze przeszkolony personel. Dobrym gwarantem powinna być, np. wdrożona norma ISO 27001. To międzynarodowa norma standaryzująca systemy zarządzania bezpieczeństwem informacji w przedsiębiorstwie. Jej wdrożenie obliguje firmy do stworzenia systemowego podejścia do zarządzania bezpieczeństwem informacji i tym samym ochrony danych powierzonych przez klientów. Roczne audyty wymuszane przez normę pilnują, żeby standardy świadczenia usług były coraz wyższe, a poziom realnego ryzyka sukcesywnie obniżany.

Procedury i ludzie u nas

Pamiętajmy jednak, że nikt nie zabezpieczy naszych danych lepiej niż my sami. Zadbajmy o to, aby odpowiednie standardy bezpieczeństwa zostały wdrożone także w naszej organizacji, aby personel obchodził się z informacjami świadomie, a także był regularnie szkolony. Regularne szkolenia są o tyle ważne, że w dzisiejszym świecie praktycznie każdego dnia może pojawić się nowy trend, który przyniesie kolejne ryzyka w zakresie bezpieczeństwa. BYOD, czyli używanie tych samych platform i narzędzi do wymiany plików w domu i w pracy to zjawiska na porządku dziennym w dzisiejszej rzeczywistości biznesowej. Tymczasem zgodnie z badaniem przeprowadzonym przez Oracle w 700 przedsiębiorstwach europejskich, aż 44% firm odczuwa dziś niechęć do zjawiska BYOD lub zezwala na jego wdrożenie jedynie w wyjątkowych okolicznościach. A to błąd, bo brak uregulowania tych kwestii w polityce bezpieczeństwa firmy oznacza, że każdy pracownik będzie stosował swoje własne zasady. Raporty firmy Coalfire nie pozostawiają złudzeń, na jakie ryzyko narażamy firmę: 47% pracowników przyznaje, że nie stosuje ochrony hasłem na swoich telefonach komórkowych, podczas gdy 84% z nich używa tych urządzeń do celów służbowych - w przypadku tabletów

ten odsetek wynosi 42%. Co ciekawe 36% osób przyznaje, że wielokrotnie używa to samo hasła, a aż 60% wciąż zapisuje hasła na kartce papieru! Ostatnio przeprowadzone przez firmę Intel Security badania ankietowe pokazały, iż trend BYOD postępuje, a jego następstwem jest większe używanie urządzeń służbowych do celów prywatnych i odwrotnie. 78% pracowników korzysta ze swych własnych urządzeń do celów służbowych, natomiast 40% respondentów korzysta z urządzeń w domu, by móc wykonać zadania służbowe. Istotnym dla analizy wynikiem jest, iż 77% pracowników podkreśla właściwe postępowanie przez pracodawcę w celu ochrony danych. Pozostaje jednak pytanie, czy polityka BYOD w tych firmach jest odpowiednio wdrażana?

Ciągłość działania i bezpieczeństwo fizyczne

Zgodnie z definicją **Aleksandry Porębskiej, Dyrektora IT w FORDATA** „*Wdrożenie i zarządzanie ciągłością działania ma na celu zapewnienie wszystkim interesariuszom – klientom, regulatorom i udziałowcom – że w razie awarii przywrócenie krytycznych funkcji biznesowych, realizowanych przez organizację nastąpi w znanym, możliwie najkrótszym czasie, i przy określonym poziomie utraty danych*". Wybierając dostawcę upewnijmy się, że także w tym obszarze posiada on odpowiednie standardy. Absolutne minimum, które powinien posiadać to plan zachowania ciągłości, plan odtwarzania systemu, współpraca z dwiema niezależnymi serwerowniami, czy regularne wykonywanie kopii zapasowych danych. Liczy się także sposób, w jaki fizycznie chronione są serwery. W naszym interesie jest sprawdzić, gdzie znajduje się serwerownia, i jakie mechanizmy bezpieczeństwa stosuje dostawca. Czy pomieszczenia serwerowni zabezpieczone są przed pożarem i innymi kataklizmami, czy mają odpowiednie systemy chłodzenia, zapewniony dostęp do alternatywnych przyłączy energetycznych oraz systemów zasilania awaryjnego, a także możliwość korzystania z infrastruktury kilku niezależnych operatorów telekomunikacyjnych.

Bezpieczeństwo sieci i aplikacji

Dla większości firm zarządzanie danymi za pomocą chmurowych rozwiązań rodzi największe obawy związane z bezpieczeństwem sieci i aplikacji. Czym zatem kierować się podczas wyboru odpowiedniego dla nas rozwiązania? Absolutnym minimum jest szyfrowanie komunikacji (SSL, najlepiej klucz 256-bitowy), odpowiednie mechanizmy uwierzytelniające (bezpieczne hasła, kody sms), automatyczne wylogowanie po określonym czasie nieaktywności, czy certyfikaty bezpieczeństwa (np. ISO). Ważne, by dane przechowywane na serwerach były domyślnie szyfrowane po stronie usługodawcy, aby firma stosowała oprogramowania antywirusowe i poddawała się regularnym testom bezpieczeństwa (m.in. symulowane ataki hackerskie, testy penetracyjne).

Dostawcy systemów chmurowych typu **Virtual Data Room** idą o krok dalej – wyposażają swoje aplikacje w takie dodatkowe mechanizmy, jak ograniczenie puli adresów IP, z których użytkownicy będą mogli logować się do systemu, czy ograniczenie ilości równoczesnych zalogowań przy wykorzystaniu tego samego loginu. Tego typu systemy służą do udostępniania poufnych dokumentów partnerom biznesowym, potencjalnym inwestorom, w wielu przypadkach firmom konkurencyjnym. Ich wyciek może rodzić bardzo poważne konsekwencje. Dlatego stosuje się takie mechanizmy, jak blokada zapisywania dokumentów na dysku, blokada drukowania, brak możliwości robienia zrzutów ekranu, czy znaki wodne na dokumentach.

Wiarygodność, czyli nie zawsze darmowe znaczy dobre

Decydując się na rozwiązanie do wsparcia krytycznych procesów biznesowych, nie możemy pominąć tego aspektu. Gdy udostępniamy najbardziej wrażliwe dane, czy realizujemy prestiżowy proces lub taki z napiętym harmonogramem, dosłownie liczy się możliwość polegania na dostawcy. W takich sytuacjach płacimy za nasz spokój ducha, za gwarancję, że dostawca rozumie nasze potrzeby i że będzie łatwo i szybko dostępny, gdy będziemy potrzebować pomocy lub wsparcia. Pamiętajmy, że darmowe najprawdopodobniej oznacza „self service".

Kontakt:
Aleksandra Prusator, e-mail: aleksandra.prusator@fordata.pl tel: 506 044 056
Beata Milewicz, e-mail: beata.milewicz@secretservices.pl tel: 508 051 138