Bezpieczeństwo danych w Data Center

Marcin Bieńkowski

W ostatnich latach coraz wyraźniej widać tendencję do rezygnowania przez firmy z własnej infrastruktury IT na rzecz usług świadczonych przez zewnętrzne centra danych. Jak wynika z raportu Telko Trendy 2015, przygotowanego przez TNS Polska na zlecenie 3S, dla 57 proc. respondentów czynnikiem zachęcającym do skorzystania z zewnętrznych serwerowni są rosnące koszty utrzymania własnej infrastruktury IT. Na drugim miejscu (47 proc.) jako przyczynę migracji wymienia się precedens utraty danych.

Przytoczone wyniki badań świadczą wyraźnie o tym, że przedsiębiorstwa coraz częściej zdają sobie sprawę z tego, że dane przechowywane w zewnętrznym centrum danych są znacznie bardziej bezpieczne niż we własnym systemie IT. Niewiele firm jest bowiem w stanie zagwarantować u siebie redundantne systemy bezpieczeństwa telekomunikacyjnego, energetycznego czy fizycznego. Rzadko też spotkać można całodobowy monitoring wszystkich krytycznych systemów IT.

Tymczasem wszystkie te elementy zapewniające znacznie większe bezpieczeństwo danych są (a przynajmniej powinny być) standardowo wdrożone w większości firm świadczących komercyjne usługi związane z przetwarzaniem danych. Dostęp do nich jest szyfrowany, nie ma więc niebezpieczeństwa, że obsługa centrum danych będzie w stanie je podejrzeć, a wykorzystanie tuneli VPN eliminuje w znacznym stopniu ryzyko podsłuchania informacji przesyłanych z firmy do centrum danych.

OCHRONA RUCHU SIECIOWEGO

– Niezależnie od tego, czy mamy do czynienia z usługami hostingu, udostępniania aplikacji czy przetwarzania informacji poufnych, ochrona informatyczna Data Center polega nie tylko na zapewnieniu bezpieczeństwa serwerom, maszynom wirtualnym czy uruchomionym na nich zasobom, ale również na osłanianiu sieci LAN. W centrum danych filtrowany jest ruch wychodzący i przychodzący przy zastosowaniu wielopoziomowego systemu zapór sieciowych. Dzięki temu można skutecznie powstrzymywać zarówno pasywne, jak i aktywne cyberataki typu DoS, DDoS, Malware, Phishing, XML attacks, Cross-Site Scripting (XSS), SQL Injection czy zapobiegać innym rodzajom zagrożeń pochodzących z zewnątrz, jak i z wewnątrz struktury Data Center. Istotnym elementem ochrony sieci jest stosowanie mechanizmów IDS/IPS umożliwiających wykrywanie ataków poprzez analizy sygnaturowe i heurystyczne – mówi Jarosław Chodkiewicz, inżynier bezpieczeństwa sieci, Bakotech.

Oprócz zapobiegania cyberzagrożeniom nie wolno zapominać również o innych czynnikach takich jak bezpieczeństwo fizyczne, środowiskowe i przeciwpożarowe w Data Center. Dostęp do obiektu, w którym znajduje się serwerownia, powinien być monitorowany na okrągło przez cały rok w trybie 24/7 przez system telewizji przemysłowej CCTV. Dostęp do obiektu powinien być podzielony na strefy, w których może przebywać jedynie autoryzowany personel. Dostęp do poszczególnych obiektów musi być kontrolowany przez specjalne czytniki oraz zabezpieczenia wykrywające otwarte drzwi.

– Jeśli chodzi o systemy bezpośredniej ochrony obszaru serwerowni, to należy sprawdzić, czy dany usługodawca ma wdrożony system klasy PSIM (Physical Security Information Management). Systemy tego typu pozwalają bowiem połączyć w jedną sprawnie działającą całość takie systemy bezpieczeństwa jak SKD (System Kontroli Dostępu), CCTV, p.poż. czy SSWiN (System Sygnalizacji Włamania i Napadu). Platforma PSIM umożliwia analizę i korelację informacji pochodzących z wielu źródeł. Dane przekazywane są do jednego punktu obsługi incydentów, w którym można (w oparciu o procedury bezpieczeństwa zaimplementowane w systemie) podjąć stosowne działania. Wszystkie te elementy pozwalają na znaczne podniesienie poziomu bezpieczeństwa chronionego obiektu – zauważa Tomasz Poręba, IT Security Consulting Director, Comarch.

POLITYKA BEZPIECZEŃSTWA

Jak widać, zapewnienie bezpieczeństwa obiektów takich jak centrum danych odbywa się na styku procedur, systemów bezpieczeństwa i czynnika ludzkiego. Wszystkie te trzy elementy muszą ze sobą poprawnie działać i to zarówno po stronie

Łukasz Pyrtko, Technical Support Manager, Diskus Polska

Należy pamiętać, że żaden z elementów tworzących data center nie zapewnia stuprocentowej pewności poprawnego działania i bezpieczeństwa danych. Jednak centra danych oferują klientowi dwa kluczowe czynniki, wpływające na poprawne działanie sprzętu IT. Są to: gwarantowane zasilanie oraz klimatyzacja. Jeśli chodzi o zasilanie, pamiętać należy o zapewnieniu jak największej liczby niezależnych jego źródeł, odpowiednim zasilaniu awaryjnym, źródłach alternatywnych oraz odpowiedniej automatyce, która sprawnie obsługiwać będzie przełączanie. Z kolei jeśli chodzi o klimatyzację, istotne jest odpowiednie odprowadzenie ciepła, tak aby urządzenia nie były narażone na awarie i uszkodzenia.

usługodawcy, jak i klienta. Na nic zdadzą się najlepsze systemy bezpieczeństwa danych w DC, jeśli poufne informacje wyniesie z firmy pracownik zatrudniony w przedsiębiorstwie klienta.

– Każdy klient ma swoją politykę bezpieczeństwa, swoje wymagania oraz swoje służby, które są odpowiedzialne za bezpieczeństwo danych. Jeżeli dostawca usług nie spełni głównych wymogów klienta, nie zostanie po prostu wybrany. Dlatego IBM, budując swoje obiekty kolokacyjne, łączy już na etapie koncepcji i projektu wszystkie elementy bezpieczeństwa fizycznego: właściwa lokalizacja obiektu, strefy, ochrona fizyczna realizowana przez najwyższej klasy komory IT oraz – rzecz jasna – procedury. Wspomniane procedury są bardzo szczegółowo zaplanowane dla każdego etapu i zdarzenia, powiązane z bezpieczeństwem fizycznym i praktycznie uniemożliwiają nieautoryzowany dostęp – zapewnia Rafał Śliwiński, Data Center Consultant Site & Facilities Solution Architect Global Technology Services, IBM.

– Co ciekawe, polityka bezpieczeństwa i waga strategicznych dla klienta danych niejednokrotnie nie pozwalają na przetrzymywanie tych danych poza siedzibą firmy. Przy takich obostrzeniach w zewnętrznych centrach danych umieszczane są mniej wrażliwe informacje. Mimo wszystko korzystanie w takiej sytuacji z usług zewnętrznego Data Center odciąża właściciela danych od konieczności znacznej rozbudowy i późniejszego utrzymania własnej infrastruktury – podkreśla Łukasz Pyrtko Technical Support Manager, Diskus Polska.

OCZEKIWANIA KLIENTÓW

– Klienci oczekują obecnie od usługodawcy przede wszystkim odpowiedniego zarządzania procesem kontroli ryzyka oraz bezpieczeństwa w odniesieniu do ich danych. Zwracają oni też uwagę na zgodność procedur i zabezpieczeń z powszechnie uznanymi standardami bezpieczeństwa (np. ISO 27001, PCI-DSS v3) lub sposobami świadczenia usług i raportowania zdarzeń (np. ISAE 3402 Type II). Często klient zleca dodatkowo u siebie niezależny audyt, który ma za zadanie zweryfikować potrzeby i procedury bezpieczeństwa, a także sprawdzić dotychczasowe środki techniczne i proceduralne oraz możliwości outsuorcingowania usług IT na zewnątrz przedsiębiorstwa – wyjaśnia Marcin Święty, IT Risk & Security Department Manager, ICT Business Unit, Comarch.

Jak dowodzą przytoczone na początku badania, użytkownicy powoli zaczynają zdawać sobie również sprawę z faktu, że profesjonalne serwerownie zapewniają większy poziom bezpieczeństwa. Wynika to przede wszystkim z tego, że skala działalności centrów danych oraz możliwość unifikacji obsługi procesów, w tym także procesów zapewnienia bezpieczeństwa, jest znacznie większa w przypadku firmy zarządzającej setkami czy tysiącami serwerów.

W ślad za rosnącym zagrożeniem atakami hakerskimi wywołanym nowymi trendami w IT (BYOD, usługi chmurowe, większa liczba urządzeń mobilnych) oraz coraz większą świadomością przedsiębiorców na temat wagi zabezpieczeń cyber security i konieczności ich stosowania powiększa się oferta produktów służących bezpieczeństwu. ABC Data podąża za tym trendem, nieustannie pracując nad powiększaniem rozległego już asortymentu z obszaru IT Security. W ostatnim czasie wprowadziliśmy do oferty nowe produkty – są to rozwiązania antywirusowe AVG Technologies, zapory sieciowe Dell SonicWALL TZ gwarantujące inspekcję przekazywanych pakietów danych czy nowe produkty z oferty firmy Symantec. Wśród produktów wybieranych przez naszych klientów najpopularniejsze są programy antywirusowe, antyspamowe i antyszpiegowskie, firewall – sieciowy bądź zintegrowany, programy antymalware, jak również coraz popularniejsze rozwiązania bazujące na chmurze.

Paweł Ryniewicz, dyrektor sprzedaży i marketingu Value+, ABC Data

Co więcej, zewnętrzne centra danych specjalizują się w dostarczaniu tego typu usług. Jest to ich główna działalność, dlatego są w stanie zatrudniać najlepszych fachowców na rynku dysponujących najwyższymi kompetencjami i wiedzą. W tych przedsiębiorstwach wykorzystuje się najnowsze rozwiązania techniczne i wysokiej klasy systemy, które są zbyt kosztowne, by wdrażać je w małych firmowych serwerowniach. Warto też zaznaczyć, że zapewnianie bezpieczeństwa danych jest również jednym z głównych zadań Data Center, dzięki temu procedury związane z bezpieczeństwem cechują się ciągłością i spójnością – co bardzo często nie jest osiągalne w środowisku wewnętrznym firmy o zupełnie innym profilu działalności. ■

Dla bezpieczeństwa danych przechowywanych w Data Center istotny jest również tzw. Disaster Recovery, czyli zbiór procedur i polityk określających postępowanie mające na celu wznowienie pracy systemu w przypadku awarii i zagwarantowanie dostępności grupy ekspertów. Plan awaryjny powinien przewidywać wiele alternatywnych scenariuszy. Wybierając Data Center należy też zainteresować się redundancją łącza internetowego, czyli liczbą niezależnych operatorów dostarczających usługę. W tym przypadku obowiązuje zasada – im więcej, tym lepiej.

Jarosław Chodkiewicz, inżynier bezpieczeństwa sieci, Bakotech