Dane cenniejsze niż kosztowności

Z Łukaszem Pyrtko, Technical Support Managerem, DISKUS Polska, rozmawia Marcin Bieńkowski

- Jakie elementy infrastruktury IT, oprogramowania, infrastruktury fizycznej oraz umiejętności personelu są obecnie najważniejsze przy zapewnieniu bezpieczeństwa dla typowej serwerowni lub centrum danych?

- Zapewnieniu bezpieczeństwa z pewnością przysłużą się dedykowane narzędzia programowe, pozwalające na badanie w czasie rzeczywistym warunków środowiskowych i stopnia obciążenia. Dzięki nim planowanie migracji czy rozbudowy infrastruktury odbywa się w bezpieczniejszy sposób.

I ostatni aspekt: czynnik ludzki – nawet najlepiej wyspecjalizowany personel nie da pewności, że nic niepożądanego się nie stanie.

- Czy fizyczne systemy zabezpieczeń, w tym zabezpieczeń przed niepowołanym dostępem do serwerowni, są równie ważne jak zabezpieczenia cyfrowe przed atakami hakerów i zabezpieczenia przed działaniem szkodliwego malware'u?

- Oczywiście. Pełna kontrola dostępu do pomieszczeń serwerowych czy nawet poszczególnych szaf to wymóg, który powinno spełniać każde profesjonalne DC. W dzisiejszych czasach dane zgromadzone w serwerowniach są niekiedy cenniejsze niż bankowe kosztowności – dlatego przemiana obiektu w fortecę nikogo w tej sytuacji nie dziwi. Z drugiej strony są też klienci, którzy wymagają od usługodawcy szeregu obostrzeń odnośnie dostępu do ich infrastruktury. Elektroniczne kody, karty dostępu, skanery tęczówki/linii papilarnych/układu żył są na porządku dziennym i również nikogo nie zaskakują. A zatem: bezpieczeństwo fizyczne jest bez wątpienia bardzo ważnym aspektem funkcjonowania obiektów klasy DC.

- Jakie obecnie zagrożenia są najbardziej niebezpieczne, jeśli chodzi o zapewnienie odpowiedniego poziomu zabezpieczenia serwerowni lub DC oraz ich nieprzerwanej pracy?

- Główne zagrożenie to zdecydowanie stabilność energetyczna – zaplanowany atak na linie przesyłowe i odcięcie lądowe obiektu mogą skutecznie wyłączyć go z użytku. Problematyczny może być także fakt dostępności wymaganej ilości mocy dostarczanej do DC – zapotrzebowanie wciąż rośnie, a niektóre rejony mają poważne deficyty produkowanej ilości energii. W tym zakresie pomoże zdecydowanie optymalizacja działania infrastruktury DC.

Innym zagrożeniem jest wcześniej już wspomniany, niemożliwy do eliminacji, czynnik ludzki.

- Jakiego poziomu bezpieczeństwa oczekują obecnie klienci powierzający swoje firmowe dane chmurowemu usługodawcy lub zewnętrznemu centrum danych?

- Oczekiwania klienta od usługodawcy są zawsze wysokie. Najlepiej, by była to forteca, tier 4, z nieskończonym zapasem energii. Rzeczywistość jednak często weryfikuje te wymagania z bardzo prostego powodu – w grę wchodzi czynnik finansowy. Wybudowanie i utrzymanie obiektu z całkowitą redundancją wszystkich systemów jest o wiele bardziej kosztowne niż w przypadku obiektu o niższym poziomie bezpieczeństwa. Do tego jeszcze należy przewidzieć wykorzystanie centrum zapasowego, które generalnie jest odbiciem centrum podstawowego.

- Dlaczego dane przechowywane w zewnętrznym centrum danych są znacznie bardziej bezpieczne? A może przeciwnie: może dane znajdujące się wewnątrz firmy są bezpieczniejsze?

- Wszystko zależy od charakteru przechowywanych danych. W 99 proc. przypadków usługodawcy wykorzystują bardzo zaawansowane techniki wykonywania kopii zapasowych.

Generalizując – nie można jednoznacznie stwierdzić, gdzie dane będą bardziej bezpieczne. Jest to uzależnione bardziej od aspektów technicznych infrastruktury własnej czy kolokacji.

- W którą stronę będą rozwijać się systemy zabezpieczeń serwerowni i centrów danych?

- Możemy się spodziewać większej automatyzacji i bardziej zaawansowanych systemów zabezpieczeń dostępowych, znanych teraz z filmów sci-fi. Szeroko pojęta integracja systemów monitoringu i bezpieczeństwa także powinna odegrać dużą rolę w podwyższeniu stopnia niezawodności systemów w DC. ■