**Chmura Windows Azure z nowym zabezpieczeniem od Barracudy**

**Platforma chmurowa Windows Azure zyskała kolejny poziom ochrony - wszystko za sprawą współpracy jaką Microsoft nawiązał z firmą Barracuda Networks, producentem rozwiązań bezpieczeństwa IT. W wyniku partnerstwa rozwiązanie Barracuda Web Application Firewall zostało wykorzystane do ochrony danych oraz aplikacji udostępnianych na platformie Windows Azure, m.in. przed atakami typu SQL injection oraz XSS, a także przed atakami polegającymi na manipulacji sesjami.**

Głównym atutem rozwiązań bazujących na chmurze jest wygoda ich używania. Z kolei największa obawa powiązana jest z bezpieczeństwem danych i aplikacji przechowywanych w chmurze - twierdzi tak aż 87% uczestników badania "Co wstrzymuje chmurę", przeprowadzonego przez Intel w maju 2012 roku. Strategiczny sojusz, jaki zawarły ze sobą firmy Barracuda Networks i Microsoft, sprawia, że obawy o bezpieczeństwo chmury stają się nieuzasadniona. Dzięki rozwiązaniu Barracude Web Application Firewall użytkownicy platformy Windows Azure zyskali taki sam poziom ochrony, jak ten, który zapewniają najlepiej zabezpieczone centra danych.

W jaki sposób działa rozwiązanie Barracuda Web Application Firewall (WAF)? Jego pracę można przyrównać do pracy moderatora, który nadzoruje komunikację pomiędzy Internetem a serwerem sieciowym. Monitorując cały ruch przychodzący i wychodzący rozwiązanie Barracudy zabezpiecza wrażliwe dane przed opuszczeniem serwera i blokuje wszelkie próby ataku, a dodatkowo chroni przed atakami typu DDoS. Warto dodać, że rozwiązanie Barracuda Web Application Firewall (WAF) nagrodzono złotym medalem SC Awards 2013 w klasie enterprise, a internauci portalu SearchSecurity wyróżnili ten produkt w kategorii "najlepszy moduł ochrony sieci".