Tomasz Łużak
T-Mobile Polska

„Reagowanie na incydenty bezpieczeństwa – szansa czy przykry obowiązek?"

Minął rok od wejścia w życie ustawy o krajowym systemie cyberbezpieczeństwa, implementującej europejską dyrektywę NIS (Network and Information Systems Directive) dotyczącą bezpieczeństwa sieci i informacji.

Na jej mocy kilkaset podmiotów zostało wpisanych do rejestru operatorów usług kluczowych. To m.in. banki, dostawcy prądu i gazu, firmy transportowe czy reprezentanci służby zdrowia. Na podmioty te zostały nałożone pewne obowiązki związane z cyberbezpieczeństwem, jak np. uruchomienie sprawnego procesu zarządzania incydentami bezpieczeństwa, pozwalającego na zgłaszanie poważnych incydentów do krajowego zespołu CSIRT.

O ile dla większych firm, które posiadają już od dawna komórki organizacyjne odpowiedzialne za bezpieczeństwo teleinformatyczne, nie powinno to stanowić poważniejszego wyzwania, o tyle mniejsze organizacje, o niższym poziomie dojrzałości w obszarze cyberbezpieczeństwa, mogą napotkać duży problem z wypełnieniem nowych ustawowych obowiązków.

Ustawa przewiduje jednak alternatywę dla tworzenia własnych, wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo – zawarcie umowy z profesjonalnym podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa – tzw. MSSP (Managed Security Service Provider).