Komisja Nadzoru Finansowego

13 kwietnia 2015 r.

**Możliwe ryzyko dla infrastruktury teleinformatycznej**

Urząd Komisji Nadzoru Finansowego (UKNF) otrzymał kierowane z Departamentu Bezpieczeństwa Teleinformatycznego w Agencji Bezpieczeństwa Wewnętrznego ostrzeżenie o możliwych w najbliższym czasie atakach na infrastrukturę teleinformatyczną.

Dlatego UKNF rekomenduje wszystkim instytucjom rynku finansowego zwrócenie szczególnej uwagi na ryzyko związane z obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego oraz pilne wdrożenie zaleceń Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL:

- Przygotowanie planu reakcji na ewentualne ataki DDoS oraz podmiany stron WWW.
- Systematyczne dokonywanie przeglądu konfiguracji kluczowych urządzeń sieciowych, znajdujących się w infrastrukturze organizacji, np. konfiguracji systemu DNS.
- Dokonanie przeglądu infrastruktury sieciowej. Zlokalizowanie elementów ograniczających transmisję. Wdrożenie reguł kontroli ruchu na urządzeniach brzegowych oraz systemach bezpieczeństwa. Przygotowanie infrastruktury pod kątem ewentualnego blokowania lub odrzucania niepożądanego ruchu sieciowego poprzez jego analizę i segregację w oparciu o zadane reguły.
- Wdrożenie dedykowanych maszyn z systemami firewall (w tym także warstwy aplikacji), IDS/IPS, monitoringu. W przypadku wystąpienia ataku eliminacja ruchu anonimizowanego. Wymuszenie ciągłej aktualizacji mechanizmów bezpieczeństwa.

- Wdrożenie algorytmów rozkładania ruchu pomiędzy wiele fizycznych lokalizacji korzystających z danych zgromadzonych lokalnie (loadbalancing). Posiadanie infrastruktury witryny www w centrum zapasowym (zalecana inna lokalizacja oraz dostawca łącza internetowego).
- Użycie mechanizmów automatycznego (oraz na żądanie) przełączenia formy wyświetlania strony (strona dynamiczna – strona statyczna – informacja o przerwie technicznej) w zależności od poziomu wysycenia łącza oraz obciążenia serwera świadczącego usługi publiczne.
- Przygotowanie umów z dostawcą łącza internetowego w kontekście zapisów umożliwiających mu podjęcie bezpośrednich działań zmierzających do odparcia ewentualnego ataku. W przypadku zlecenia świadczenia usługi obsługi strony firmie zewnętrznej istotne jest zawarcie odpowiednich zapisów w umowie umożliwiających podjęcie samodzielnych działań w celu zniwelowania zagrożenia w przypadku jego wystąpienia. Należy uwzględnić również odpowiedzialność firmy hostującej za zapewnienie ciągłości działania powierzonego serwisu, a w przypadku operatora zapewniającego jedynie połączenie – minimalną gwarantowaną przepustowość łącza.