

Możliwe ryzyko dla infrastruktury teleinformatycznej instytucji sektora finansowego

Urząd Komisji Nadzoru Finansowego (UKNF) otrzymał od Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL informację o możliwych w najbliższym czasie atakach na infrastrukturę teleinformatyczną instytucji sektora finansowego.

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 ataki odmowy świadczenia usług (DDoS), w tym wyznaczenie osób odpowiedzialnych za kontakty z dostawcami usług internetowych.
- 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. 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 sposób umożliwiający mu podjęcie bezpośrednich działań zmierzających do odparcia ewentualnego ataku. W przypadku zlecenia świadczenia usługi obsługi strony firmie zewnętrznej, zaleca się przygotowanie odpowiednich zapisów w umowie, umożliwiających jej podjęcie działań w celu zniwelowania zagrożenia w przypadku jego wystąpienia. Wprowadzenie odpowiedzialności firmy hostującej za zapewnienie ciągłości działania powierzonego serwisu, a w przypadku operatora zapewniającego jedynie połączenie – minimalną gwarantowaną przepustowość łącza.