Cyberbezpieczeństwo

Firma ATM S.A. z siedzibą w Warszawie, ul. Grochowska 21a, zgodnie z decyzją Ministerstwa Infrastruktury została uznana za operatora usługi kluczowej jako podmiot prowadzący punkt wymiany ruchu internetowego (IXP), stanowiący obiekt sieciowy, który umożliwia połączenie międzysystemowe pomiędzy więcej niż dwoma niezależnymi systemami autonomicznymi, głównie do celów ułatwienia wymiany ruchu internetowego. Warunek wynikający z ustawy to co najmniej 100 podłączonych systemów autonomicznych, licząc średniorocznie, biorąc pod uwagę średnią z ostatnich 3 lat.

W związku z powyższym informujemy, że jako operator usługi kluczowej dokładamy wszelkich niezbędnych starań w celu zapewnienia ciągłości działania usługi kluczowej zgodnie z wymaganiami ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560), jak również zapewnienia naszym klientom dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową.

ATM S.A. stawia na podejście procesowe i bezpieczeństwo informacji, a tym samym zaangażowanie w codzienne wspieranie i promowanie działań mających wpływ na skuteczność procesów oraz odpowiednie zabezpieczenie przetwarzanych informacji, w tym określenie szans i ryzyk, przeprowadzenie analizy i wdrożenie działań doskonalących i zabezpieczających.

Spółka działa w oparciu o system zarządzania bezpieczeństwem informacji zgodny z normą ISO/IEC 27001. Głównym z założeń systemu jest szacowanie ryzyka, w tym ryzyka wystąpienia zagrożeń mających niekorzystny wpływ na proces świadczenia usługi kluczowej, a docelowo wdrożenie działań minimalizujących prawdopodobieństwo ich wystąpienia.

Spółka wdrożyła odpowiednie procedury i zasady działania w obszarach takich jak:

- Niedostępność lub awaria usługi kluczowej

  Wskazane działy biorące udział w realizacji/utrzymaniu usług mają dostęp do stale aktualizowanych instrukcji postępowania.

- Podział odpowiedzialności za poszczególne obszary systemu

  Poszczególne role i odpowiedzialności przydzielone w ramach realizacji i utrzymania usługi Thinx IX zostały jasno zdefiniowane.

- Konfiguracja sieciowa, adresacja i architektura rozwiązania

  Dokumentacja stanowiąca opis architektury rozwiązania jest utrzymywana i stale aktualizowana.

  Do realizacji usługi Thinx IX użyto urządzeń klasy operatorskiej, które mają zapewnioną opiekę serwisową. Architektura rozwiązania minimalizuje wpływ ewentualnej awarii na jakość usługi świadczonej klientowi.

- Kryteria i warunki skorzystania z usługi, ruch dozwolony w ramach Thinx IX

  Na interfejsie/VLAN-ie wpiętym do Thinx IX klient musi mieć skonfigurowaną tylko adresację przydzieloną przez Atmana (przynależną do Thinx IX).

Klient jest zobowiązany, żeby ruch kierowany do Thinx IX był adresowany tylko do klientów Thinx IX. Ramki powinny zawierać jedną z poniższych wartości ethertype:

- 0x0800 – IPv4
- 0x0806 – ARP
- 0x86dd – IPv6

- Zarządzanie poziomem uprawnień i dostępem do systemów i urządzeń

Dostęp administracyjny do urządzeń sieciowych ograniczony jest do wyznaczonych zespołów. Uprawnienia są cyklicznie weryfikowane, a ich poziom jest uzależniony od poziomu wiedzy i doświadczenia administratora.

- Ochrona przed atakami DDoS

Ochrona przed atakami DDoS jest zrealizowana z wykorzystaniem Blackholingu. Blackholing działa w trybie passive stand-by i w przypadku wystąpienia ataku nie wymaga zmian konfiguracyjnych po stronie ATM S.A. Klient obserwujący atak na swoją infrastrukturę ma możliwość rozgłoszenia zaatakowanego prefiksu, oznaczonego specjalnym atrybutem community BGP, do route serwerów węzła, a niepożądany ruch zostanie przekierowany na urządzenie, które będzie automatycznie unieszkodliwiać ten ruch.

- Dodatkowe zabezpieczenia

Prefiks węzła 212.91.0.0/22 nie jest rozgłaszany do sieci Internet, dzięki czemu ograniczona została możliwość ataku DDoS na urządzenia wpięte do węzła.

Zgodnie z wytycznymi ustawy, jeżeli zauważą Państwo coś niepokojącego, co ma związek z cyberprzestępczością, prosimy o poinformowanie o tym fakcie stosowne służby:

1. Zgłaszanie incydentów naruszających bezpieczeństwo w sieci
2. Przyjmowanie zgłoszeń dotyczących nielegalnych treści w Internecie