Cyberbezpieczeństwo

ATM S.A. dokłada wszelkich niezbędnych starań w celu zapewnienia ciągłości działania usługi Thinx IX 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 Thinx IX.

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 procedury i zasady działania w oparciu o międzynarodowe standardy ISO/IEC 27001 oraz ISO 22301 w obszarach takich jak:

- Monitorowanie ciągłości działania komponentów usługi Thinx IX

  Zespół NOC (Network Operations Center) zapewnia nieprzerwane monitorowanie ciągłości działania wszystkich komponentów usługi Thinx IX w trybie 24/7/365. Monitorowanie pozwala zarządzać problemami technicznymi i identyfikować potencjalne naruszenia bezpieczeństwa. Zespół Zarządzania Incydentem zapewnia odpowiednią reakcję na wystąpienie incydentu bezpieczeństwa.

- Niedostępność lub awaria usługi kluczowej

  Opracowano i testuje się plany postępowania na wypadek awarii lub niedostępności poszczególnych komponentów usługi Thinx IX. Zapewnia się wymianę wiedzy i doświadczeń w ramach doskonalenia postępowania kryzysowego.

- 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. Audyty i weryfikacje prowadzone przez wykwalifikowanych inżynierów

zapewniają odpowiednią konfigurację i minimalizują ryzyko wystąpienia błędów bezpieczeństwa czy podatności.

- 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 ATM S.A. (przynależną do Thinx IX).

Klient jest zobowiązany, żeby ruch kierowany do Thinx IX był adresowany tylko do klientów Thinx IX.

- Zarządzanie poziomem uprawnień i dostępem do systemów i urządzeń

Dostęp administracyjny do urządzeń sieciowych ograniczony jest do wyznaczonych pracowników. 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.

Warstwowy model bezpieczeństwa obejmuje również konfigurację rozwiązania klienckiego.

ATM S.A. jako dostawca usługi zapewnia szereg systemów protekcji (zarówno organizacyjnych, jak i teleinformatycznych). Jednak z naszego doświadczenia wynika, że bezpieczeństwo każdej z usług sieciowych jest wprost proporcjonalne do zabezpieczenia najsłabszego ogniwa. Dlatego tak ważna jest odpowiednia konfiguracja urządzeń klienckich, które wykorzystują usługę Thinx IX.

- Redundancja

Klienci powinni korzystać z usług dwóch niezależnych operatorów. W przypadku całkowitej niedostępności usługi świadczonej przez jednego z operatorów druga zapewnia ciągłość działania.

- Szyfrowanie połączeń

Ważnym aspektem jest również bezpieczne łącze transmisji danych w warstwie drugiej modelu ISO/OSI (L2) pomiędzy dwiema lokalizacjami, szyfrowane np. np. przy pomocy protokołu MACsec.

- Monitoring łącza – jak wykrywać nieprawidłowości i potencjalne ataki DoS/DDoS?

Klienci w aplikacji Strefa Klienta Atman, która znajduje się pod adresem https://strefaklienta.atman.pl/, mają dostęp do statystyk ruchu w zadanym przedziale czasowym: rocznym, miesięcznym, tygodniowym, dziennym, godzinowym lub we wskazanym przez użytkownika zakresie (z dokładnością do jednej minuty). Dzięki tej funkcji klienci mogą śledzić wysycenie łącza i w razie konieczności modyfikować konfigurację własnych komponentów sieci lub zlecać upgrade usługi. Ponadto zaleca się umożliwienie analizy NetFlow po stronie klienta, która zapewnia dokładne informacje o miejscu, rodzaju i sile ataku. Nie do przeceniania są także zabezpieczenia takie jak IDS/IPS, a także monitorowanie wykorzystania poszczególnych komponentów infrastruktury sieciowej.

Zgodnie z wytycznymi ustawy, jeżeli zauważą Państwo coś niepokojącego, co ma związek z cyberprzestępczością, prosimy o kontakt e-mailowy lub telefoniczny:

- servicedesk@atman.pl
- 22 51 56 800

Dodatkowo możliwe jest poinformowanie o tym fakcie stosownych służb:

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