Urządzenia sieciowe – bezpieczeństwo

Poniższa informacja ma zastosowanie do urządzeń MAZi, ReviZOOM, Abaxo, CNB a także do innych urządzeń posiadając dostęp do Internetu.

1. Możliwe zagrożenia

W ostatnim czasie obserwujemy rosnącą popularność wszelkiego rodzaju narzędzi do wyszukiwania aktywnych urządzeń sieciowych, skanowania portów, skryptów do automatycznego logowania a także narzędzi do ataków typu brute force.
Na tego typu ataki narażone są wszystkie urządzenia podłączone do sieci niezależnie od marki i rodzaju.

2. Przyczyny udanego ataku

Zazwyczaj atakujący testuje tylko najbardziej popularne hasła (np. 12345, 1111, admin, root) oraz porty (np. zakres 80-89, 21, 25, 443, 554).
Niestety wielu użytkowników pozostawia porty oraz hasła standardowe.
W takim wypadku można bardzo łatwo, po wykryciu że pod danym adresem jest urządzenie, sprawdzić czy np. na porcie 80 jest widoczny web-serwer albo 21 telnet.
Jeśli tak to atakujący może próbować logowania się na rejestrator czy kamerę.

3. Skutki udanego ataku

Skutkiem udanego zalogowania może być zmiana haseł dostępowych, ingerencja w ustawienia rejestratora, czy nawet usunięcie danych.

4. Zapobieganie zagrożeniom

Zapobieganie polega na:

- stosowaniu skomplikowanych haseł, absolutne minimum to
  - 8 znaków oraz zastosowanie równocześnie
  - duże litery
  - małe litery
  - cyfry
  - symboli specjalnych
- zmiana portów
  - ze standardowych na inne, koniecznie powyżej 1024
  - unikanie stosowania portów o typowych, prostych kombinacjach cyfr np. 8080
- nie udostępnianiu urządzeń poprzez umieszczaniu w DMZ
- przekierowywanie tylko niezbędnych portów
- jeśli urządzenie posiada taką funkcję (np. nowe urządzenia MAZi) to włączamy blokowanie po nieudanym logowaniu lub kilku kolejnych nieudanych logowaniach. Wtedy następna próba logowania możliwa jest dopiero po określonym czasie, zazwyczaj 20 minut
- aktualizacja firmware'u do najnowszej dostępnej wersji

Obowiązkiem użytkownika jest dbanie o prawidłowe zabezpieczenie urządzeń przed niepowołanym dostępem.