ZALECENIA BEZPIECZEŃSTWA SIECIOWYCH URZĄDZEŃ CCTV

ul. Poprzeczna 8
55-050 Sobótka

71 332 92 00 do 05

biuro@xrplus.pl

W ostatnim czasie obserwujemy wzmożone ataki hakerskie na różnego rodzaju komputery i serwery. Ryzyko ataków hakerskich dotyczy wszystkich urządzeń podłączonych do Internetu, w tym również rejestratorów cyfrowych i kamer IP. Wiele urządzeń pada ofiarami ataków, ponieważ lekceważone są kwestie związane z bezpieczeństwem. W celu zminimalizowania ryzyka uszkodzenia rejestratorów i kamer w wyniku ataku hakerskich zalecamy zastosowanie się do poniższych wskazówek.

ZMIANA DOMYŚLNYCH HASEŁ W URZĄDZENIACH

Zalecamy zmianę domyślnych haseł zarówno w routerze, jak również rejestratorach i kamerach. Stosowanie haseł typu "admin", "123456" itd. ułatwia nieautoryzowany dostęp zdalny. Hasła powinny być trudne do odgadnięcia i zawierać różne znaki i cyfry. Dobrą praktyką jest tworzenie odrębnych haseł dla każdego użytkownika i dbanie o to, by dostęp do urządzeń sieciowych miały tylko upoważnione osoby. Zaleca się również okresową zmianę haseł.

REZYGNACJA Z FUNKCJI DMZ W ROUTERZE

DMZ to tzw. strefa zdemilitaryzowana i umieszczenie w niej urządzenia sieciowego daje dostęp z sieci zewnętrznej do wszystkich portów jakie są otwarte w konfiguracji domyślnej. Jest to bardzo niebezpieczna sytuacja, ponieważ większość konfiguracji ma domyślnie otwarty port TELNET, który wykorzystywany jest do większości ataków hakerskich. Zalecamy całkowitą rezygnację z funkcji DMZ dla wszystkich urządzeń sieciowych i przekierowywanie tylko niezbędnych do pracy portów na routerze.

ZMIANA DOMYŚLNYCH PORTÓW

Najczęściej atakowanym przez hakerów jest domyślny port 80. Zalecamy zmianę domyślnych portów HTTP / TCP / UDP dla wszystkich urządzeń pracujących w sieci, co utrudni ich odgadnięcie przez osoby trzecie.

RACJONALNIE ZARZĄDZANIE UŻYTKOWNIKAMI

Sugerujemy ustawianie odrębnych haseł dla każdego użytkownika oraz szczególną dbałość o to, by nikt niepowołany

nie posiadał dostępu do żadnego z urządzeń sieciowych. Zaleca się rezygnację z automatycznego logowania i każdorazowe wprowadzanie haseł do urządzeń i programów sieciowych.

STAŁA ADRESACJA URZĄDZEŃ

Sugerujemy rezygnację z funkcji DHCP i ustawianie stałej adresacji wszystkich urządzeń pracujących w sieci. Jeśli to możliwe, to zalecamy uruchomienie filtrów MAC / IP, dzięki czemu wskażemy zaufane urządzenia, które mogą się połączyć z routerem.

DEDYKOWANE SIECI DO INSTALACJI CCTV

Dobrą praktyką jest tworzenie wydzielonych sieci tylko dla systemów monitoringu, w których nie ma innych urządzeń o swobodnym dostępie zdalnym. Warto również wspomnieć, że sam rejestrator powinien znajdować się w zabezpieczonym miejscu, do którego nie mają dostępu osoby trzecie (serwerownie, skrzynie zabezpieczające do rejestratorów).