Wyższa Szkoła Technologii Informatycznych w Katowicach

# REFERAT PRACY DYPLOMOWEJ

**Temat pracy:** Projekt i implementacja sieci kablowo-bezprzewodowej w środowisku heterogenicznym z uwzględnieniem aspektów bezpieczeństwa

**Autor:** Przemysław Galicki

**Promotor:** dr hab. inż. Dariusz Badura

*Kategorie: bezpieczeństwo sieci*

*Słowa kluczowe: 802.1Q, RADIUS, DoH, Firewall*

## 1. Cel i podstawowe założenia

Głównym celem pracy jest osiągnięcie wysokiego poziomu bezpieczeństwa rozpatrywanej sieci kablowo-bezprzewodowej, łączącej wysoko zróżnicowane urządzenia klienckie, takie jak: komputery, urządzenia mobilne, urządzenia sfery IoT oraz urządzenia gościnne z poza organizacji. Realizacja celu wymaga zaprojektowania i wdrożenia nowej struktury logicznej sieci, oraz zastosowania logicznych i technicznych metod zaradczych uniemożliwiających przełamanie zabezpieczeń sieci, czy to w wyniku ataku hakerskiego czy też w wyniku błędów ludzkich wynikających z nieświadomości użytkowników.

## 2. Realizacja projektu

W ramach pracy przeprowadzono analizę istniejącej infrastruktury dostępowej pod względem podatności na ataki sieciowe i wspierane metody zabezpieczeń, jak również analizę urządzeń klienckich pod względem: rodzajów urządzeń, wykorzystywanego medium transmisyjnego, zastosowań i ról pełnionych w sieci, wrażliwości przetwarzanych przez nie danych, oraz wspieranych metod autentykacji dostępu do sieci Wi-Fi. Analiza ujawniła szereg problemów w zakresie konfiguracji sieci obejmujących m.in.:

- możliwość wzajemnej niekontrolowanej komunikacji pomiędzy wszystkimi urządzeniami klienckimi w wyniku braku segmentacji w warstwie 2 modelu OSI, oraz braku kontroli przekazywania pakietów w warstwie 3.
- stosowanie niewystarczających metod autentykacji i autoryzacji dostępu do sieci bezprzewodowej spowodowane brakiem polityki silnych haseł, brakiem wdrożonych mechanizmów filtrowania urządzeń podłączających się do sieci, oraz brakiem składników wymaganych dla stosowania najsilniejszej metody uwierzytelniania EAP-TLS.
- podatność klientów sieci na ataki typu MITM dla zapytań protokołu DNS
- podatność infrastruktury na wprowadzenie do sieci nieautoryzowanych serwerów DHCP
- podatność infrastruktury na ataki typu DOS
- stosowanie niewystarczających zabezpieczeń dostępu do zarządzania infrastrukturą sieciową
- wykorzystanie routera brzegowego nie posiadającego wsparcia w zakresie aktualizacji oprogramowania systemowego.
- wykorzystanie routera brzegowego nie wspierającego standardu 802.11ac

Analiza przedwdrożeniowa wykazała iż głównym czynnikiem sprawczym znalezionych problemów jest kluczowy element infrastruktury jakim jest przestarzały router sieciowy. W kolejnych krokach dokonano przeglądu dostępnych technologii umożliwiających rozwiązanie występujących problemów wraz ze sformułowaniem założeń projektowych które je eliminują. Pozwoliło to na określenie wymagań funkcjonalnych które stały się podstawą do wyboru nowego rozwiązania sprzętowego spełniającego te wymagania. Na tej podstawie wykorzystując nowy router MikroTik HAP AC^2 wdrożono schemat segmentacji sieci grupujący podobne urządzenia w strefach bezpieczeństwa pod postacią sieci VLAN, uzyskując w ten sposób pożądaną separację klientów przetwarzających wrażliwe dane prywatne od niosących ryzyko urządzeń sfery IoT, wydzielono również osobną podsieć zarządzania infrastrukturą sieciową. Wdrożono funkcjonalność DHCP-Snooping w celu ochrony przed nieautoryzowanymi serwerami DHCP. Z powodzeniem objęto segmentacją część bezprzewodową sieci tworząc wirtualne BSS dla poszczególnych kategorii urządzeń, Skonfigurowano również bezpieczną usługę dostępu do Internetu dla klientów zewnętrznych poprzez wdrożenie sieci gościnnej wraz z mechanizmem wzajemnej izolacji klientów.

Z sukcesem wdrożono kontroler sieci bezprzewodowej CAPsMAN, oferując możliwość rozszerzania zasięgu sieci Wi-Fi, oraz umożliwiając wygodne, centralne zarządzanie, dołączanymi zgodnymi AP. Na potrzeby uwierzytelniania metodą EAP-TLS wdrożono opartą na minikomputerze Raspberry Pi 4 instancję serwera FreeRADIUS. Wykorzystanie uwierzytelniania opartego na certyfikatach w znaczący sposób podniosło bezpieczeństwo klientów WLAN przetwarzających krytyczne dane, uniemożliwiając w praktyce przełamanie zabezpieczeń sieci bezprzewodowej z wykorzystaniem zarówno ataków bazujących na podsłuchiwaniu, jak również ataków typu MITM. Uwolniło to klientów od konieczności pamiętania haseł oraz wyeliminowało konieczność ich regularnych zmian, uniemożliwia to również przekazanie danych dostępowych do sieci osobom trzecim. W odniesieniu do klientów uwierzytelniających się za pomocą kluczy WPA2-PSK określono politykę złożoności haseł po czym, dla urządzeń IoT wdrożono mechanizm indywidualnych poświadczeń, a dla sieci gościnnej, wykorzystując wbudowany interpreter skryptów, automatyczną okresową zmianę hasła dostępowego, wysyłanego pocztą e-mail do zainteresowanych stron. Jako dodatkowe zabezpieczenie dostępu do sieci bezprzewodowej zaimplementowano reguły filtrowania adresów MAC podłączanych klientów wraz z wymuszeniem asocjacji z pożądanym BSS, uzyskując pełną kontrolę nad tym kto, gdzie się łączy. Jako główny element kontroli przekazywania pakietów pomiędzy wirtualnymi sieciami lokalnymi skonfigurowano pełnostanową zaporę sieciową. Reguły zapory utworzono zgodnie z metodyką zero-trust, uzyskując gwarancje że tylko pożądany, zgodny z założeniami ruch będzie przepuszczany. W celu ochrony klientów przed atakami MITM na pakiety protokołu DNS wdrożono globalne dla wszystkich podsieci wykorzystanie DoH, wraz z dodatkowymi mechanizmami ochrony i filtrowania, świadczonymi przez wybranego dostawcę usługi OpenDNS. W zakresie utrzymania aktualnej wersji oprogramowania systemowego routera, wdrożono sterowany harmonogramem skrypt powiadamiania administratora o dostępnych aktualizacjach, a na potrzeby awaryjnego przywracania konfiguracji, skrypt tworzenia i wysyłania kopii aktualnych ustawień z wykorzystaniem poczty e-mail. Aby uniemożliwić nieautoryzowane logowanie do routera skonfigurowano restrykcyjne reguły dostępu oraz zmieniono porty sieciowe znanych usług. Wdrożenie zakończono przeprowadzając konfigurację dodatkowych elementów obejmujących usługę serwera synchronizacji czasu oraz zapasową instancję serwera FreeRADIUS w postaci maszyny wirtualnej.

## 3. Produkt końcowy

W efekcie bieżącej pracy powstała sieć komputerowa w bezpieczny sposób łącząca medium kablowe i radiowe. Spełnia ona współczesne, wynikające z postępującej heterogenizacji urządzeń sieciowych wymogi w zakresie dostępu, segmentacji oraz kontroli przepływu danych. Zastosowany elastyczny schemat adresowania, oraz wdrożony kontroler sieci bezprzewodowej zapewniają jej łatwą rozbudowę i wysoką skalowalność.

## 4. Informacje o możliwości wykorzystania / wykorzystaniu pracy

Zrealizowane wdrożenie można zastosować w większości kablowo-bezprzewodowych sieci komputerowych segmentu SOHO. Głównymi ograniczeniami są wydajność sprzętowa wybranego routera oraz koszty pracy administratora związane z generowaniem, instalowaniem i wycofywaniem certyfikatów urządzeń klienckich.