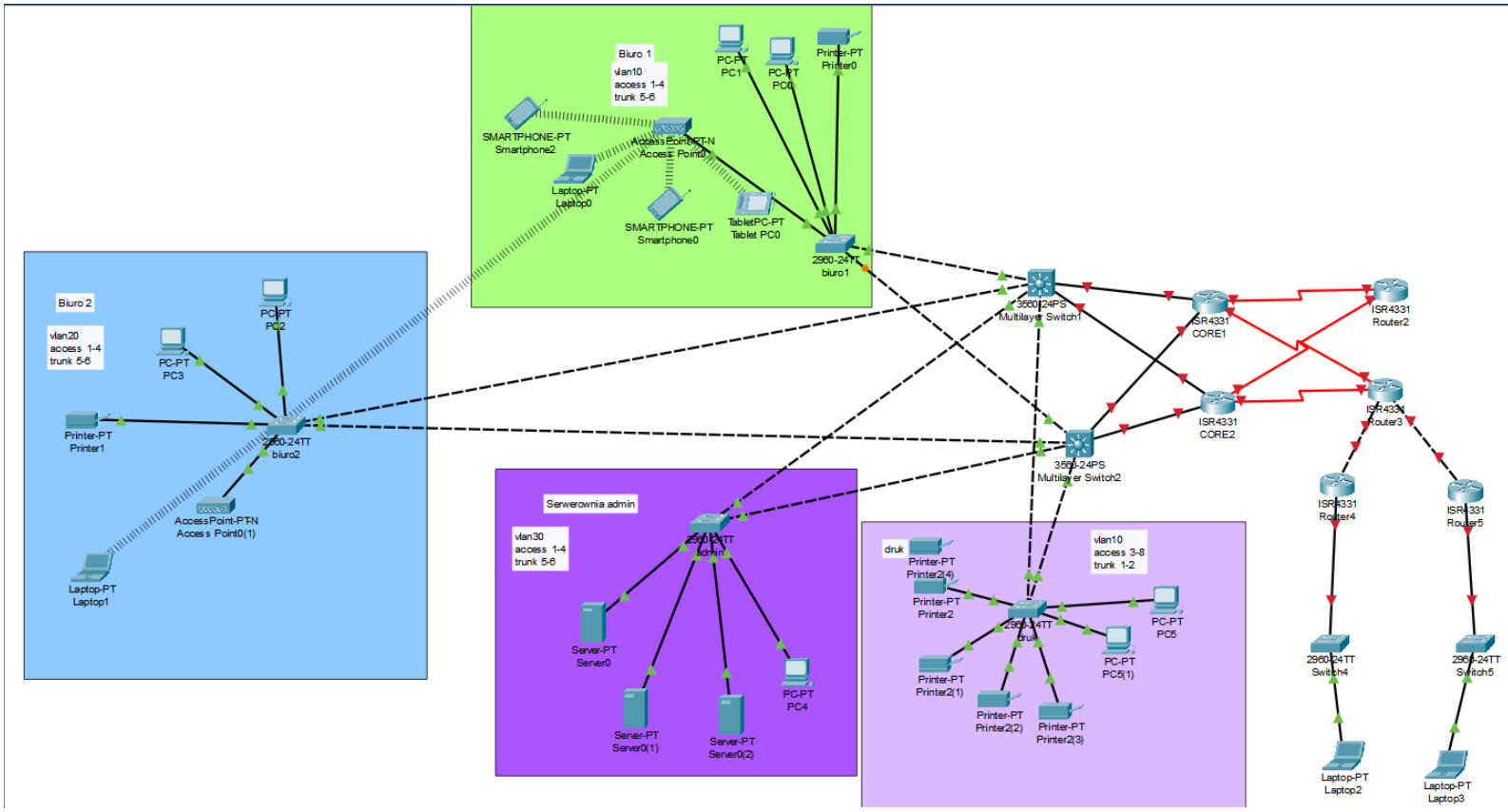
Politechnika Świętokrzyska w Kielcach Wydział Elektrotechniki, Automatyki i Informatyki		
PROJEKT : Bezpieczeństwo Infrastruktury Sieciowej		
Temat: Urząd gminy	**Zespół**: Adam Rzepka, Bartłomiej Tokar, Michał Mosiołek **Grupa**: 1ID24B	**Data oddania sprawozdania**: 13.11.2023 r.

1. Topologia sieci



Opis topologii:

Topologia została wykreowana na wzór sieci utworzonej dla urzędu Gminy. Pomieszczenie Biuro 1 oraz Biuro 2 są podobne. Znajdują się tam komputery dla pracowników oraz access pointy dla urządzeń mobilnych. W pokoju serwerownia admin znajduje się serwer DHCP który będzie umożliwiał hostom uzyskanie od serwera danych konfiguracyjnych, np. adresu IP. Kolejnym pomieszczeniem jest Druk. Znajdują się tam dwa komputery oraz podłączone do sieci drukarki. Switche wychodzące z pokoi łączą się z multilayerowymi switchami. Switche łączą się z routerami CORE które mają połączenie z dostawcą usług internetowych ISP. Obok znajduje się podsieć na której zaprezentujemy działanie IPSEC VPN.

2. **Opis możliwych zagrożeń**

Nieautoryzowany dostęp:

Atakujący może próbować uzyskać dostęp do sieci lub urządzeń, wykorzystując słabe hasła lub błędy w konfiguracji. Może to prowadzić do nieautoryzowanego dostępu do danych lub infrastruktury sieciowej.

Utrata dostępu do urządzenia:

Utrata dostępu do kluczowych urządzeń, takich jak serwery lub routery, może wynikać z awarii sprzętu lub ataków. To może prowadzić do przerw w świadczeniu usług lub utraty danych.

Awaria urządzenia:

Awarie urządzeń sieciowych mogą być spowodowane problemami sprzętowymi, przeciążeniem lub błędami w konfiguracji. Mogą prowadzić do przerw w działaniu sieci lub usług.

Ataki sieciowe typu MAC:

Ataki typu MAC mogą obejmować podszywanie się pod adresy MAC urządzeń, co pozwala na nieautoryzowany dostęp do sieci. Ataki te mogą zakłócić działanie sieci i skierować ruch na złośliwe serwery.

Ataki DDoS (Distributed Denial of Service):

Ataki DDoS polegają na przeciążeniu sieci lub usług poprzez generowanie ogromnej ilości ruchu. To może spowodować przerwy w działaniu usług i spadek wydajności sieci.

Próba łamania haseł do dostępu SSH za pomocą brute force:

Atakujący może próbować złamać hasła dostępowe do usług SSH, takie jak zdalny dostęp do serwerów. Jeśli hasła są słabe, atakujący może uzyskać nieautoryzowany dostęp do urządzeń.

3. **Obrona przed zagrożeniami.**

Aby zabezpieczyć sieć przed tymi zagrożeniami, można podjąć następujące kroki:

- Wdrożyć silne hasła i autoryzację dwuetapową, aby zabezpieczyć dostęp do urządzeń.
- Regularnie aktualizować oprogramowanie i firmware urządzeń sieciowych.
- Monitorować ruch sieciowy i stosować zabezpieczenia przed atakami DDoS.
- Konfigurować mechanizmy bezpieczeństwa, takie jak listy dostępu, zapory ogniowe i systemy wykrywania włamań.
- Edukować personel w zakresie świadomości bezpieczeństwa i praktyk bezpieczeństwa.
- Warto także zwrócić uwagę na lokalne przepisy i regulacje dotyczące ochrony danych i bezpieczeństwa sieci w urzędzie gminy, aby zapewnić zgodność z obowiązującymi przepisami.