Kielce, 03.11.2023 r.

Bezpieczeństwo infrastruktury sieciowej

Projekt: Księgarnia

Autor: Aleksandra Kwiatkowska

Wiktoria Sikora

Grupa:1ID24B

Spis treści

[**1.** **Wprowadzenie** 3](#_Toc149909286)

[**2.** **Topologia** 3](#_Toc149909287)

[**3.** **Zagrożenia** 3](#_Toc149909288)

# **Wprowadzenie**

Dokumentacja zawiera szczegółowe informacje dotyczące infrastruktury sieciowej, architektury, konfiguracji i zarządzania siecią w ramach księgarni. Przedstawimy tutaj zasady działania sieci oraz poszczególnych komponentów.

# **Topologia**

Sieć można podzielić na Budynek\_A oraz Budynek\_B. Zarówno w pierwszym budynku jak i drugim występuje sieć hierarchiczna, a dokładniej sieć dwuwarstwowa. Posiadamy warstwę dostępu, która pozwala aby urządzenia końcowe mogły korzystać z sieci. Druga warstwa pełni funkcję warstwy dystrybucji oraz rdzenia, czyli operuje całym ruchem w sieci oraz umożliwia dostęp do i z Internetu. Każdy VLAN posiada PC oraz znajdują się również drukarki, smartfony czy laptopy. Budynek\_A oraz Budynek\_B posiadają po dwa rutery oraz przełączniki dystrybucji, które mają za zadanie, w razie awarii jakiegoś urządzenia, przejąć ich pracę.

W Budynek\_A występuje następująca adresacja:

* VLAN 10 (name HR): 192.168.10.0/24
* VLAN 20 (name Księgowosc): 192.168.20.0/24
* VLAN 30 (name Obsluga\_klienta): 192.168.30.0/24
* VLAN 99 (name Admin\_A): 192.168.99.0/24
* VLAN 40 (name Serwerownia): 192.168.40.0/24

Budynek\_B:

* VLAN 50 (name Administracja): 192.168.50.0/24
* VLAN 60 (name Sklep): 192.168.60.0/24
* VLAN 70 (name Admin\_B): 192.168.70.0/24
* VLAN 80 (name Zamowienia): 192.168.80.0/24

Gateway\_A połączony jest z Gateway\_B: 10.0.0.4/30   
Gateway\_A połączony jest z Gateway\_C: 10.0.0.0/30   
Gateway\_D połączony jest z Gateway\_B: 10.0.0.8/30   
Gateway\_D połączony jest z Gateway\_C: 10.0.0.12/30

# **Zagrożenia**

Sieć mogą czekać następujące zagrożenia:

* **Ataki zero-day** - to ataki wykorzystujące niedawno odkryte luki w oprogramowaniu. Regularne aktualizacje oprogramowania i monitorowanie ruchu sieciowego mogą pomóc w wykryciu i obronie przed takimi atakami.
* **Ataki DDoS** - to rodzaj cyberataku, w którym grupa atakujących komputerów lub urządzeń sieciowych współpracuje, aby zalać celowaną stronę lub usługę z dużą ilością zapytań lub ruchu internetowego, co ma na celu spowodowanie zakłóceń lub całkowitej niedostępności usługi. Atak DDoS jest nazwany "rozproszonym", ponieważ jest wykonywany z wielu źródeł, co utrudnia zidentyfikowanie i zneutralizowanie atakujących.
* **Ataki wewnętrzne** - to zagrożenia, które wywodzą się od pracowników, dostawców lub innych osób, które mają dostęp do wewnętrznych zasobów organizacji. Ataki wewnętrzne mogą być celowe lub wynikać z nieostrożności lub błędów, ale zawsze stanowią poważne ryzyko dla bezpieczeństwa organizacji.
* Ataki na warstwę fizyczną sieci to próby naruszenia samej infrastruktury sieciowej, czyli komponentów sprzętowych, które stanowią jej fundament. Ataki tego typu mogą mieć poważne konsekwencje, ponieważ wpływają na dostępność sieci i mogą prowadzić do przerw w działaniu.
* Ataki społeczne, takie jak phishing, to techniki manipulacji psychologicznej, które atakują naszą ludzką naturę, by uzyskać poufne informacje, hasła, dane osobowe lub dostęp do systemów. Ataki te polegają na oszukiwaniu użytkowników w celu wyłudzenia cennych informacji lub wykonywania niepożądanych działań.