**Bezpieczeństwo sieci teleinformatycznych**

**Prowadzący: Dr inż. Marcin Markowski**

**Wykonali:**

Tomasz Borusiewicz, 219278

Bartłomiej Bednarz,

Michał Polek,

1. **Wstęp**
   1. **Cel projektu**

Celem projektu jest opracowanie kompleksowej dokumentacji bezpieczeństwa teleinformatycznego dla firmy “Lex Consulting” zwanego dalej zleceniodawcą. W skład dokumentacji wchodzić będzie: analiza ryzyka, określenie wymagań projektowych, ogólna polityka bezpieczeństwa, plan bezpieczeństwa teleinformatycznego oraz plany odtwarzania ciągłości działania.

* 1. **Charakterystyka firmy**

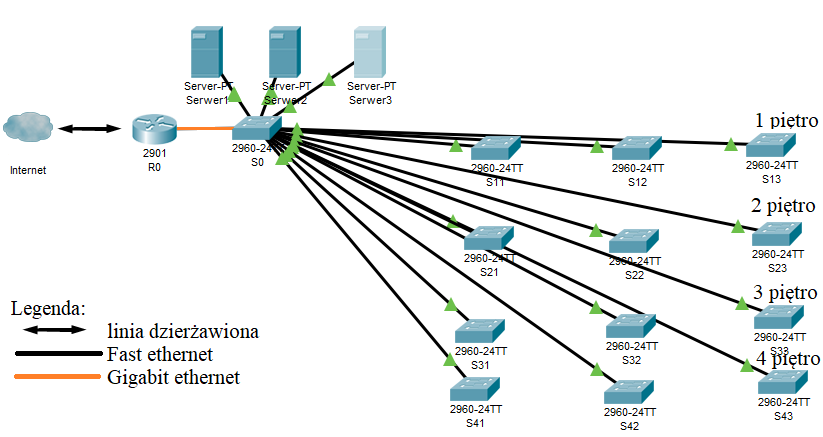
Poniżej opisana została charakterystyka firma dla której wykonana zostanie dokumentacja bezpieczeństwa teleinformatycznego.

**Profil działalności instytucji**

Przedsiębiorstwo mieści się przy ulicy Polnej 2 we Wrocławiu w budynku “Red Tower”. Zajmuje kolejno pierwsze, drugie, trzecie oraz czwarte piętro. Biuro prawne “Lex Consulting” zajmuje się kompleksową obsługą klientów z zakresu dziedzin prawnych. Zakres oferowanych usług obejmuje między innymi:

* Doradztwo prawne,
* Konsultacje i doradztwo, opiniowanie wniosków,
* Przygotowywanie wniosków o dofinansowania lub preferencyjne pożyczki dla osób zamierzających założyć własną działalność gospodarczą,
* Opracowanie wniosków o dofinansowanie ze środków unijnych i krajowych,
* Zarządzanie projektami,
* Szkolenia z zakresu prawa pracy, prawa cywilnego i prawa administracyjnego.
  1. **Zasoby informatyczne i struktura sieci**

W pomieszczeniach zajmowanych przez zleceniodawcę istnieje sprawna instalacja telefoniczna, energetyczna oraz okablowanie strukturalne w postaci nieekranowanego kabla (UTP) kategorii 6. Struktura sieci stworzona została w topologii gwiazdy, która obejmuje 13 przełączników warstwy drugiej, router, 3 serwery oraz 240 punktów abonenckich. Firma posiada specjalnie wydzielony pokój na pierwszym piętrze w którym umiejscowione został punkt dystrybucyjny, router oraz serwerownia, w pomieszczeniu tym znajduję się także punkt styku sieci lokalnej z siecią rozległą. Przedsiębiorstwo posiada trzy serwery z którym dwa służą do przechowywania danych firmy oraz aplikacji niezbędnych do prowadzenia działalności. Trzeci serwer zapewnia usługi WWW oraz pełni rolę serwera poczty. Wszystkie serwery są dostępne z Internetu poprzez przekierowanie portów na routerze. Oprócz sieci przewodowej istnieje także punkt dostępowy sieci WiFi znajdujący się w sali konferencyjnej zabezpieczony za pomocą szyfrowania WEP. Struktura sieci pokazana została na poniższym rysunku (rys.1) :



Rys. 1 - Struktura sieci firmy "Lex Consulting"

1. **Analiza ryzyka**

Jednym z pierwszych elementów które należy wykonać podczas projektowania bezpieczeństwa sieci jest analiza ryzyka, w celu jasnego określenia modelu zarządzania ryzykiem. Głównym zadaniem analizy ryzyka jest zidentyfikowanie krytycznych zasobów, które należy ocenić i wyznaczyć koszty naruszenia tych zasobów. Następnie można ocenić dopuszczalny stopień ryzyka dla firmy oraz określić przeciwdziałania potencjalnym zagrożeniom.

* 1. **Inwentaryzacja i identyfikacja zasobów**

Inwentaryzacja i identyfikacja zasobów w przedsiębiorstwie pozwoli na określenie poziomu, który trzeba przeznaczyć na zapewnienie bezpieczeństwa. Zasoby podzielono na informacyjne oraz teleinformatyczne. Przedstawiają je poniższe tabele:

|  |  |  |  |
| --- | --- | --- | --- |
| **Typ zasobu** | **Rodzaj zasobu** | **Szczegóły** | **Liczebność** |
| Bazy danych | dane pracowników,  dane klientów,  dane finansowe, | dane dotyczące pracowników,  dane dotyczące klientów,  dane finansowe firmy | - |
| Dane | Kopie zapasowe | tworzenie / aktualizacja / usuwanie  kopi zapasowych | - |
| Dokumentacja | dane administracyjne  dane badawcze,  dane zastrzeżone | kartoteki,  procedury biurowe,  tendencje rynkowe  materiały szkoleniowe,  firmowe podręczniki użytkownika,  patenty,  tendencje rynkowe,  umowy,  firmowe dokumentacje systemu,  tokeny uwierzytelnia | - |
| Sprzęt  (“zasoby fizyczne”) | stacja robocza,  router,  switch,  router WiFi  serwer, | dokładniejszy opis w punkcie 2.2 | 120  1  13  1  3 |
| Oprogramowanie | system operacyjny, | System operacyjny Microsoft Windows 10 Home PL 64-bit OEM  Windows Server 2019 Essentials | 120  3 |
| oprogramowanie użytkowe, | MySQL Enterprise Edition  Pakiet Office 2019 Home and Business | 120 |
| oprogramowanie antywirusowe, | Avast 2018 | 120 |

* 1. **Identyfikacja zasobów o znaczeniu kluczowym**
  2. **Identyfikacja zagrożeń i podatności**
* Upublicznienie danych klientów
  + jako celowe działanie pracownika
  + błąd pracownika
  + działanie zewnętrzne
* Skasowanie danych z bazy danych
  + celowe
  + przypadkowe
* Awarie sprzętowe
* Kradzież danych i szpiegostwo korporacyjne
  + wewnętrzne
  + zewnętrzne
* Podatności wynikającego z nieaktualnego oprogramowania
* Podatności wynikające z czynnika ludzkiego
  + Phishing - otwarcie zainfekowane maila
  + Podłączenie zainfekowanego pendrive
  + Pobranie zainfekowanie pliku
  1. **Szacowanie ryzyka**

W szacowaniu prawdopodobieństwa wystąpienia danej podatności korzystamy z następującej skali:

|  |  |  |
| --- | --- | --- |
| Poziom | Opis | Prawdopodobieństwo |
| 4 | Bardzo prawdopodobne | > 50% |
| 3 | Prawdopodobne, znane są liczne przypadki wystąpienia | 10–50% |
| 2 | Średnio prawdopodobne. Znane są przypadki wystąpienia | 2–10% |
| 1 | Mało prawdopodobne. Nieznane lub znane pojedyncze przypadki wystąpienia | 0–2% |

|  |  |
| --- | --- |
| **Podatność** | **Ryzyko** |
| Upublicznienie danych klientów | |
| jako celowe działanie pracownika | **2** |
| błąd pracownika | **3** |
| działanie zewnętrzne | **1** |
| Skasowanie danych z bazy danych | |
| celowe | **1** |
| przypadkowe | **2** |
| Awarie sprzętowe |  |
| Kradzież danych i szpiegostwo korporacyjne | |
| wewnętrzne | **2** |
| zewnętrzne | **1** |
| Podatności wynikającego z nieaktualnego oprogramowania | **3** |
| Podatności wynikające z czynnika ludzkiego | |
| Phishing - otwarcie zainfekowane maila | **3** |
| Podłączenie zainfekowanego pendrive | **3** |
| Pobranie zainfekowanie pliku | **3** |

* 1. **Opracowanie scenariuszy testów penetracyjnych**

Testy penetracyjne są to symulowane ataki przeprowadzane na zlecenie. Ich zadaniem jest wykrycie podatności bez narażania zleceniodawcy na starty. Zazwyczaj przeprowadzany przez niezależne podmioty.

**Test penetracyjny - skanowanie portów.**

1. Zainstalowanie programu NMAP.

2. Przeprowadzenie skanowania komputerów w sieci wraz z ich otwartymi portami poprzez wprowadzenie komendy: *nmap -T5 192.168.1.0/24*

3. Wyszukanie potencjalnie otwartych portów na serwerze: *nmap --open 192.168.1.0*

1. **Określenie wymagań projektowych**

Rozwiązanie zaproponowane w tym projekcie mają na celu zwiększenie bezpieczeństwa teleinformatycznego sieci. Długofalowa polityka przedsiębiorstwa zlecającego dąży do dbania o dobre imię firmy poprzez ciągłe doskonalenie jakości usług, a także zapewnienie bezpieczeństwa i poufności danych klientów, co jest niezwykle istotne podczas prowadzenia działalności o takim charakterze.

Projekt uwzględnia doposażenie firmy w sprzęt zapewniający niezawodność, bezpieczeństwo oraz jakość świadczonych usług.

**Podstawowe założenia koncepcyjne:**

* Tworzenie VLAN w zwiększenia bezpieczeństwa danych w sieci (802.1Q)
* Zapewnienie bezpieczeństwa przesyłu danych w sieci poprzez zastosowanie szyfrowania
* Scentralizowany system nadzoru, zatrudnienie osoby na stanowisku administratora sieci oraz regularna aktualizacja oprogramowania.
* Zapewnienie komunikacji pomiędzy urządzeniami w warstwie sieciowej
* Zapewnienie kontroli dostępu do sieci – serwer RADIUS 802.1X
* Serwer kopii zapasowej

Szkolenia korporacyjne dotyczące bezpieczeństwa sieciowego

1. **Ogólna polityka bezpieczeństwa**
2. **Plan bezpieczeństwa teleinformatycznego**
3. **Plany odtwarzania ciągłości działania**