Politechnika Poznańska
Wydział Elektryczny
Instytut Automatyki i Inżynierii Informatycznej

Maciej Marciniak 121996
Dawid Wiktorski 122056

Projekt zarządzania bezpieczeństwem sieciowego systemu przechowywania danych

prowadzący:
mgr inż. Michał Apolinarski

Poznań, 2017

Spis treści

Wstęp

Projekt zarządzania bezpieczeństwem sieciowego systemu przechowywania danych polega na zaproponowaniu rozwiązań mających na celu zabezpieczenie systemu, zarządzania nim oraz w jaki sposób przechowywać dane. Zabezpieczaną firmą jest biuro rachunkowe, której właścicielami są Krzysztof Łuczak oraz Damian Filipowicz.

W pracy najpierw zostanie przedstawiony stan wejściowy firmy, biuro które jest tylko częściowo zabezpieczone przez właścicieli budynku. W następnym rozdziale zostanie przeprowadzony audyt bezpieczeństwa, mający na celu oszacowanie potencjalnych zagrożeń systemów.

1 Opis zabezpieczanej firmy

Rozdział zawiera charakterystykę firmy, rodzaj prowadzonej działalności, plan budynku oraz spis sprzętu i pracowników. Jest to stan biura sprzed zabezpieczenia.

1.1 Charakterystyka firmy

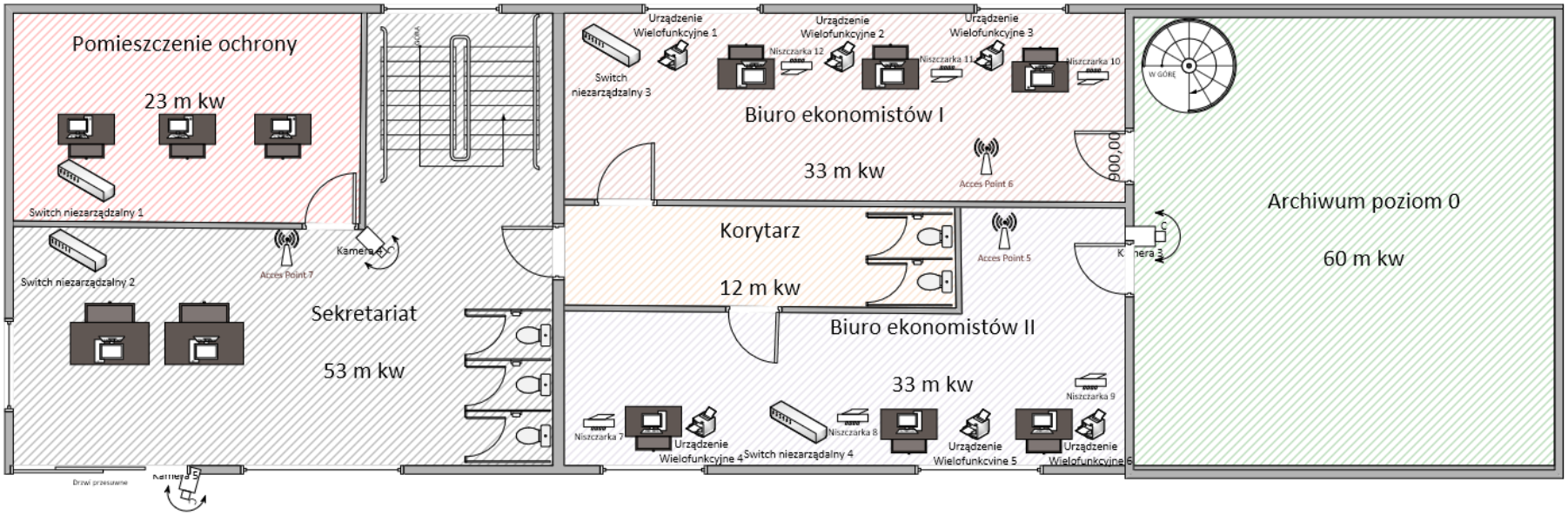
Firma jest biurem rachunkowym specjalizującym się w doradztwie finansowym, prowadzaniu księgowości dla przedsiębiorstw oraz przygotowywaniu analizy finansowej rynku. Przedsiębiorstwo zatrudnia 39 osób, które tworzą cztery działy: dział ekonomistów, dział sprzedaży, dział IT i dział obsługi.

1.2 Opis budynku

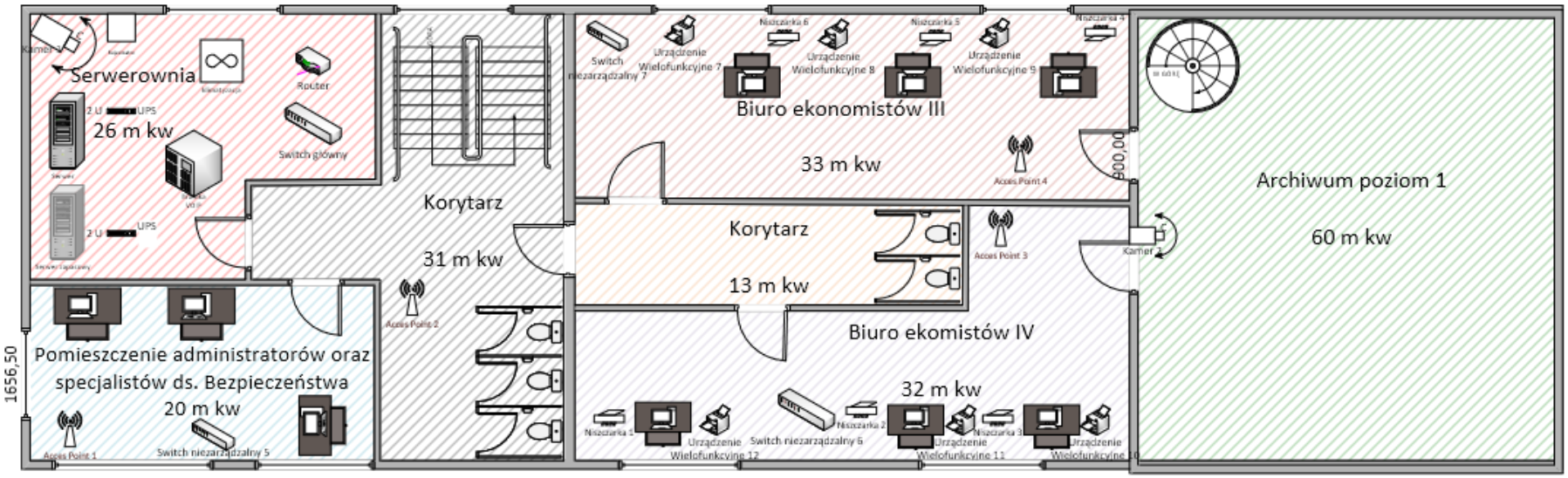
Dwupiętrowy budynek firmy zlokalizowany jest na obrzeżach dużego miasta. W okolicy jest pomijalnie niskie ryzyko wystąpienia klęsk żywiołowych. Budynek otaczają stare drzewa, których nie można wyciąć, ponieważ objęte są ochroną gatunkową. Do przedsiębiorstwa doprowadzona jest sieć telefoniczna oraz internetowa.

Pomieszczenia w budynku zostały zaprojektowane bez uwzględnienia podłogi technicznej, ani sufitu podwieszanego. Urządzania typu routery (Access Point), switche, kamery, alarmy itp. zostały zamontowane na ścianie lub bezpośredniość w suficie. Przewody zasilające oraz sieciowe poprowadzone są w listwach wzdłuż ścian.

Schemat rozmieszczenie pomieszczeń na parterze i piętrze znajduje się odpowiednio na Rys. 1 i 2.



Rys. 1: Układ pomieszczeń na parterze



Rys. 2: Układ pomieszczeń na piętrze

1.3 Sprzęt oraz oprogramowanie

Poniżej wymieniony został sprzęt informatyczny znajdujący się w firmie wraz z jego podstawowymi parametrami:

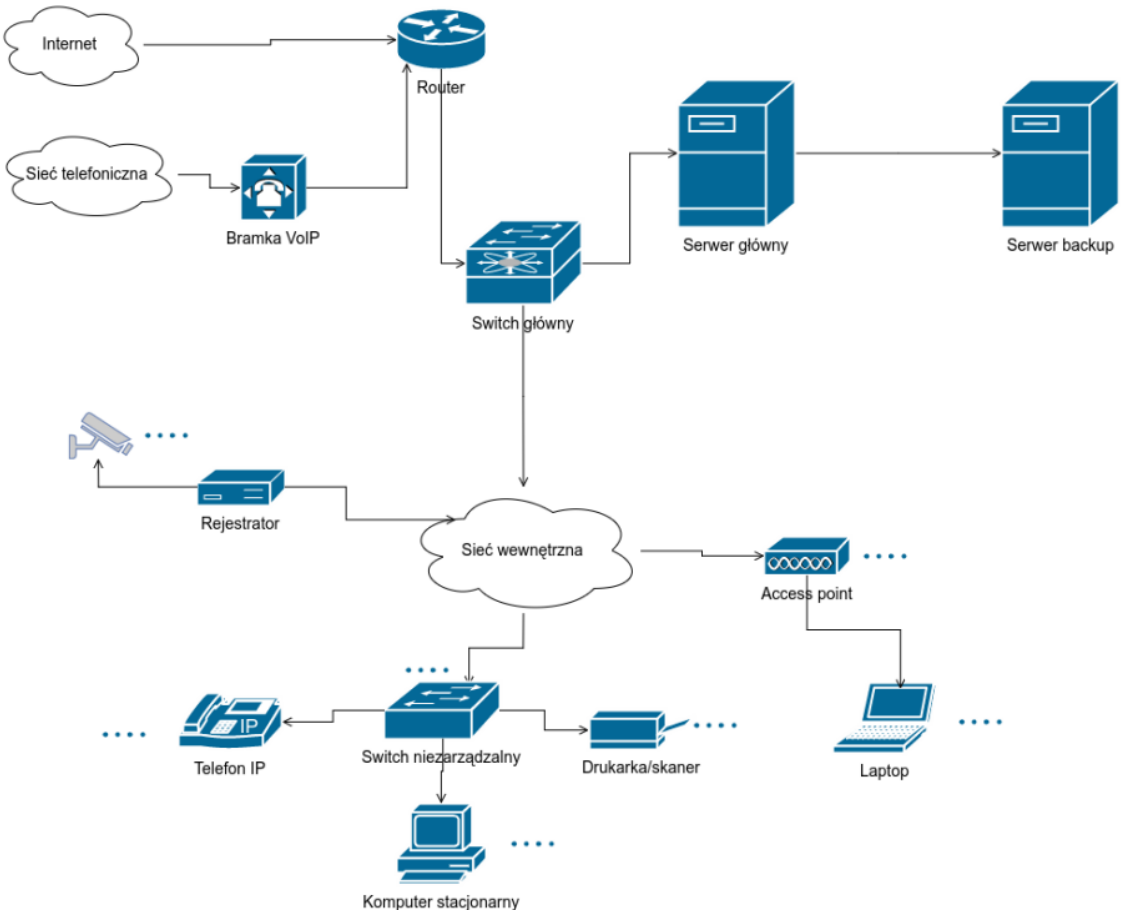
- urządzenie wielofunkcyjne Canon PIXMA G3400 (12 sztuk),
- niszczarka ProfiOffice PIRANHA EC 7 CC (12 sztuk),
- komputer stacjonarny (21 sztuk):
  - procesor Intel i5,
  - pamięć 8 GB RAM DDR3,
  - dysk 1 TB HDD,
- laptop DELL Inspiron 5567 (dział IT 6 sztuk),
- telefon VoIP Cisco CP-7940G (21 sztuk),
- laptop DELL Inspiron 5567 (6 sztuk),
- serwer główny (1 sztuka):
  - płyta główna: Intel S2600CP4,
  - procesor Intel Xeon e5-2603 v2,
  - pamięć 128 GB RAM DDR3,
  - dyski SSD o łącznej pojemności 40 TB,
- serwer zapasowy (1 sztuka):
  - płyta główna: Intel S2600CP4,
  - procesor Intel Xeon e5-2603 v2,
  - pamięć 16 GB RAM DDR3,
  - dyski SSD o łącznej pojemności 10 TB,
- router Cisco RV325 (1 sztuka),
- switch główny Cisco SG300-52 (1 sztuka),
- bramka VoIP Grandstream HT704 (1 sztuka),
- switch niezarządzalny Cisco SB SF100D-16EU (7 sztuk),
- punkt dostępowy Asus RP-AC87 (7 sztuk),
- okablowanie:
  - między serwerami 1 Gb/s,
  - w pozostałych połączeniach skrętka 100 Mb/s,
- UPS VOLT Micro 1200 (1 sztuka),
- monitoring:
  - rejestrator BCS-P-QDVR0801ME z dyskiem 2 TB HDD (1 sztuka),
  - kamera LV-IP2301IP (5 sztuk),
- taśmy magnetyczne.

Poniżej znajduje się spis oprogramowania (licencji) jakie jest zainstalowane w komputerach:

- komputery pracowników w dziale ekonomistów:
  - Windows 10 (18 sztuk),
  - pakiet Office 2016 (18 sztuk),
  - pakiet Insert GT (18 sztuk),
  - Windows Defender (18 sztuk),
- komputery sekretariatu i działu sprzedaży:
  - Windows 10 (3 sztuk),
  - pakiet Office 2016 (3 sztuk),
  - Windows Defender (3 sztuk),
- komputery pracowników w dziale IT:
  - Windows 10 (6 sztuk),
  - pakiet Office 2016 (6 sztuk),
  - pakiet Insert GT (6 sztuk),
  - Windows Defender (6 sztuk),
- oprogramowanie serwera i wykorzystywane technologie:
  - Linux Ubuntu 16.04 LTS z OpenStack (umożliwia wirtualizację dowolnego systemu),
  - bazy danych MSSQL,
  - bazy danych MySQL,
  - OpenVPN,
  - Windows Server 2016 (5 sztuk),
  - Linux Debian 8,
  - Pakiet Insert GT (sztuk),
  - system pocztowy Exim i Dovecot:
    - Roundcube jako klient poczty w przeglądarce.

1.4 Schemat sieci informatycznej

Sieci informatyczna składa się z routera do którego podłączony jest Internet (poprzez światłowód), switcha głównego, 7 switchy niezarządzanych, centrali VoIP oraz 7 punktów dostępowych. Schemat sieci przedstawiony jest na Rys. 3. Oznaczenie trzech kropek symbolizuje możliwość podpięcia wielu urządzeń do sieci.



Rys. 3: Schemat sieci informatycznej

Adresacja sieci:

- Router — brama VoIP — switch główny:
  - Adres sieci: 192.168.0.0,
  - Maska sieci: 255.255.255.0,
- Switch główny — serwer główny:
  - Adres sieci: 192.168.1.0,
  - Maska sieci: 255.255.255.0,
- Switch główny — access pointy — urządzenia podłączone przez WiFi:
  - Adres sieci: 192.168.2.0,
  - Maska sieci: 255.255.255.0,
- Switch główny — rejestrator:
  - Adres sieci: 192.168.3.0,
  - Maska sieci: 255.255.255.0,
- Switch główny — urządzenia podłączone do switchy niezarządzalnych:
  - Adres sieci: 192.168.4.0,
  - Maska sieci: 255.255.255.0,

1.5 Organizacja pracy

1.6 Przechowywane dane

2 Identyfikacja zagrożeń i analiza ryzyka

W niniejszym rozdziale zostanie przeprowadzony audyt bezpieczeństwa. Zostaną przedstawione potencjalne zagrożenia m systemie.

Jednym z zagrożeń jest możliwość upadku drzewa na budynek firmy, co może spowodować pożar lub utratę prądu. W przypadku pożaru istnieje duże ryzyko utraty danych, ponieważ żadne z pomieszczeń nie posiada systemu przeciwpożarowego. Prawdopodobieństwo wystąpienia upadku drzewa na budynek obecnie jest stosunkowo niskie. Natomiast, trzeba wziąć pod uwagę zmieniający się klimat w Polsce, który w przyszłości będzie sprzyjał powstawaniu silnych wiatrów, a tym samym prawdopodobieństwo wystąpienia tego zjawiska będzie coraz większe.

Następnym zagrożeniem jest włamanie się do budynku. Zadanie nie jest trudne, ponieważ w oknach nie są stosowane alarmy, zamki na klucz czy też kraty, które utrudniłyby dostanie się do budynku. Również, drzwi nie są specjalnie zabezpieczone, a więc włamywacz przy pomocy, np. wytrychu jest w stanie w łatwy sposób dostać się do każdego pomieszczenia. Prawdopodobieństwo wystąpienia fizycznego włamania do budynku jest na średnim poziomie.(lub średnio-wysokim?). Skutki mogą być poważne. Włamywacz nie tylko może ukraść sprzęt/dane, ale także może zainstalować oprogramowanie szpiegujące.

W komputerach pracowników używany jest Windows Defender, który nie jest tak skuteczny przeciwko wirusom jak produkty konkurencji. W przypadku gdy, użytkownik pobierze zainfekowany plik, istnieje średnie prawdopodobieństwo, że zawirusowany zostanie komputer czy też inne urządzenia podłączone do sieci.

Hackerzy mają ułatwione zadanie związane z dostaniem się na serwery dlatego, że w serwerach nie jest używane dodatkowe oprogramowanie związane z bezpieczeństwem. Nie ma też sprzętowej zapory ogniowej, która filtrowałaby cały ruch sieciowy.