Politechnika Poznańska
Wydział Elektryczny
Instytut Automatyki i Inżynierii Informatycznej

Projekt zarządzania bezpieczeństwem sieciowego systemu przechowywania danych

Twórcy:
Maciej Marciniak 121996
maciej.r.marciniak@student.put.poznan.pl
Dawid Wiktorski 122056
dawid.wiktorski@student.put.poznan.pl

Właściciele firmy:
Damian Filipowicz 122002
damian.filipowicz@put.poznan.pl
Krzysztof Łuczak 122008
krzysztof.t.luczak@student.put.poznan.pl

Specjalność: Bezpieczeństwo systemów informatycznych2017/2018 semestr VII

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.

Następny rozdział przedstawia propozycje przechowania danych. System uwzględnia dostęp do danych poprzez intranet oraz ma mieć na celu maksymalną minimalizację podatności na uszkodzenia sprzęt.

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

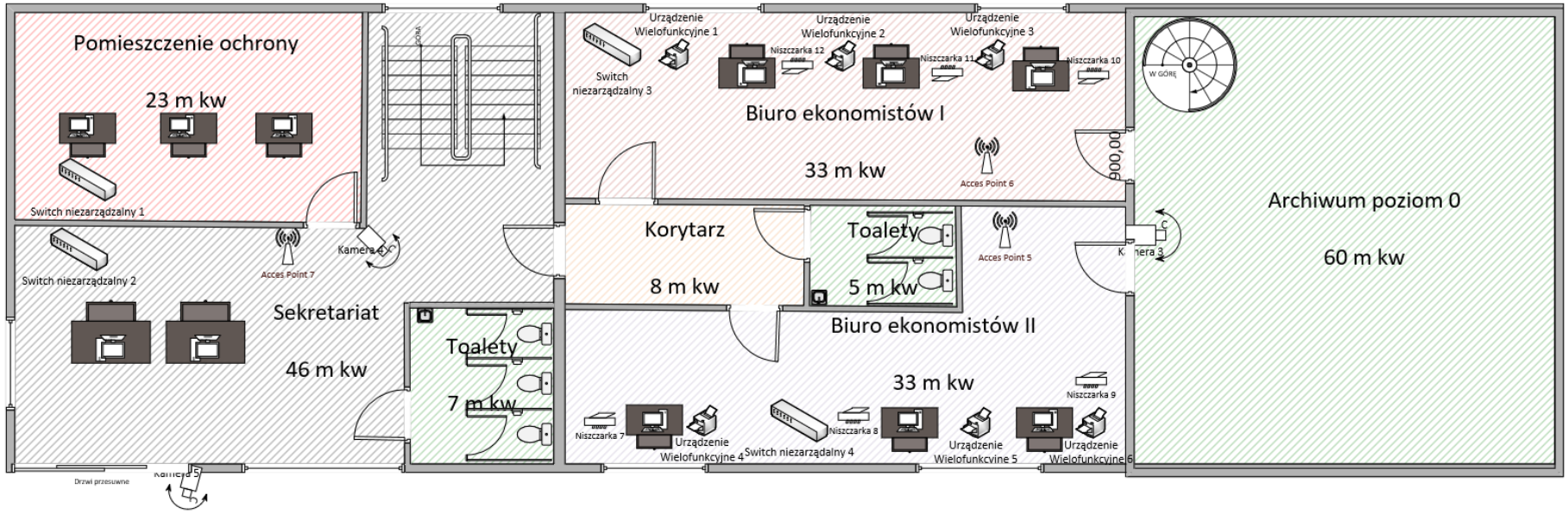
Firma jest biurem rachunkowym specjalizującym się w doradztwie finansowym, prowadzaniu księgowości dla przedsiębiorstw oraz przygotowywaniu analizy finansowej rynku. Przedsiębiorstwo zatrudnia 42 osoby, które tworzą cztery działy: dział ekonomistów, dział sprzedaży, dział IT i dział obsługi.

1.2 Opis budynku

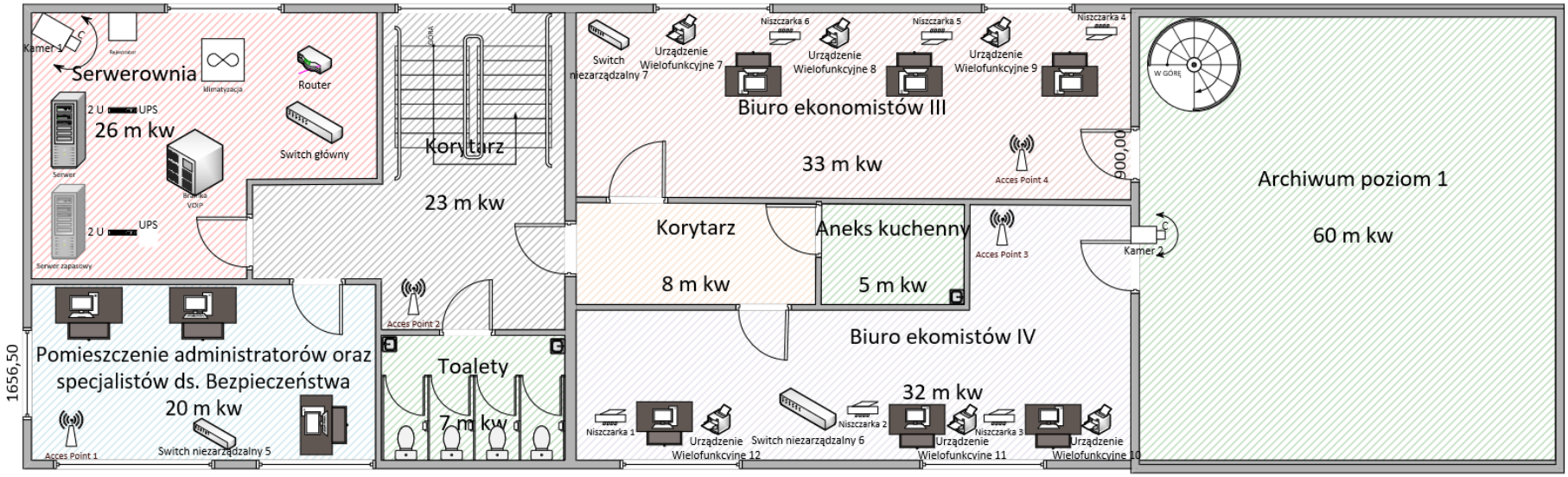
Dwupiętrowy budynek firmy zlokalizowany jest na obrzeżach dużego miasta. W okolicy jest pomijalnie niskie ryzyko wystąpienia klęsk żywiołowych. Budynek otaczają stare drzewa, których nie można wyciąć, ponieważ objęte są ochroną gatunkową. Do przedsiębiorstwa doprowadzona jest sieć telefoniczna oraz internetowa.

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

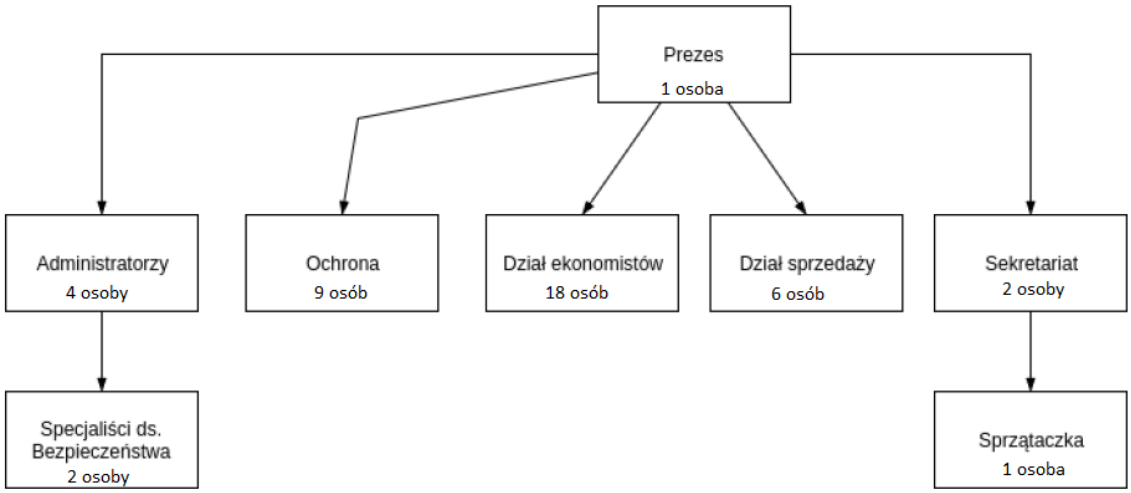
1.3 Organizacja pracy

W firmie zatrudnionych bezpośrednio jest 32 osób. Dodatkowo 10 osób pochodzi z wynajętych zewnętrznych firm (9 ochroniarzy oraz 1 sprzątaczka). Łącznie w budynku pracuje na zmiany 42 osoby. Biura otwarte są od 6.00 do 22.00, przy czym obowiązują następujące zasady zmian:

- Administratorzy pracują w zmianach 6:00-14:00 i 14:00-22:00 (po 2 na zmianę),
- Specjaliś ci ds. bezpieczeństwa pracują w zmianach 6:00-14:00 i 14:00-22:00 (po 1 na zmianę),
- Ochrona pracuje całodobowo w zmianach 12h z 24h przerwą, pracownicy ochrony zmieniają się w godzinach 4:00 i 16:00(po 3 na zmianę),
- Pracownicy sekretariatu pracują od 8:00- 16:00 (po 2 na zmianę),
- Dział ekonomistów pracuje w zmianach 6:00-14:00 i 14:00-22:00 (po 9 na zmianę),
- Dział sprzedaży pracuje w zmianach 6:00-14:00 i 14:00-22:00 (po 3 na zmianę),
- Sprzątaczka przychodzi w niedzielę, wtorek czwartek o godzinie 22:00.

Pracownicy ochrony podpisują politykę prywatności, mając przy tym dostęp do wszystkich pomieszczeń budynku, wraz z archiwum. Ochroniarz co godzinę po zamknięciu biur przeprowadza obchód po terenie firmy.

Hierarchia pracowników przedstawiona jest na Rys. 3.



Rys. 3: Hierarchia pracowników

1.4 Sprzęt oraz oprogramowanie

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

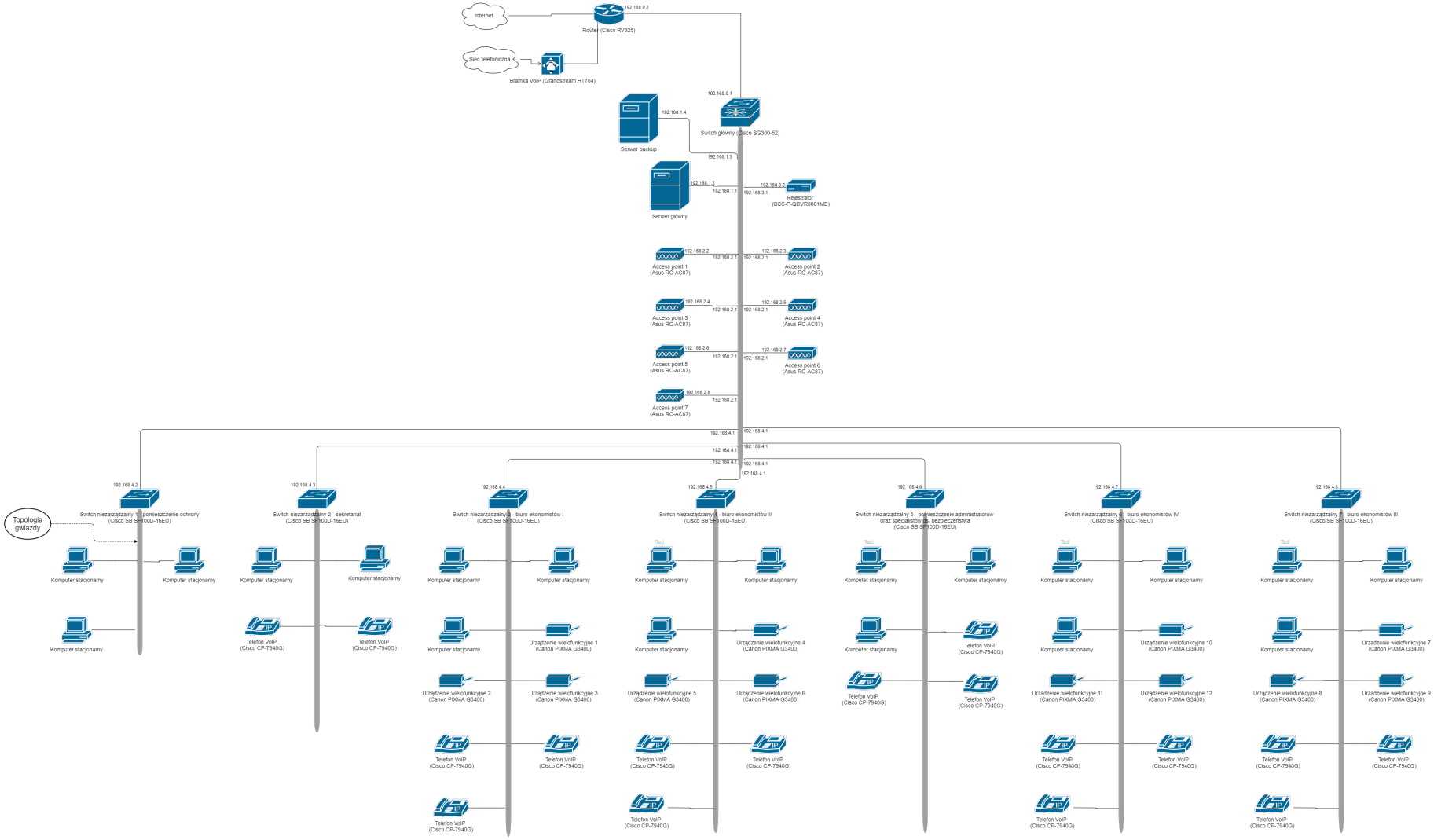
- urządzenie wielofunkcyjne Canon PIXMA G3400 (12 sztuk),
- niszczarka ProfiOffice PIRANHA EC 7 CC (12 sztuk),
- komputer stacjonarny (18 sztuk):
  - procesor Intel i5,
  - pamięć 8 GB RAM DDR3,
  - dysk 1 TB HDD,
  - myszka, klawiatura, monitor 24",
- laptop DELL Inspiron 5567 (dział IT 6 sztuk),
- monitor ochrony 24"(2 sztuki),
- telefon VoIP Cisco CP-7940G (17 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 skrętka kategorii SF/FTP 7A (40 Gb/s),
  - pozostałe połączenia skrętka kategorii U/UTP 6 (200 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 (9 sztuk),
  - pakiet Office 2016 (9 sztuk),
  - pakiet Insert GT (9 sztuk),
  - Windows Defender (9 sztuk),
- komputery sekretariatu, ochrony i działu sprzedaży:
  - Windows 10 (6 sztuk),
  - pakiet Office 2016 (6 sztuk),
  - Windows Defender (6 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),
  - Pakiet Insert GT (5 sztuk),
  - system pocztowy Exim i Dovecot: Roundcube jako klient poczty w przeglądarce.

1.5 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. 4. Oznaczenie trzech kropek symbolizuje możliwość podpięcia wielu urządzeń do sieci.



Rys. 4: Schemat sieci informatycznej

1.6 Przechowywane dane

Przechowywane dane użytkowe znajdują się na dyskach twardych w komputerach oraz na serwerze. Pliki archiwalne oraz kopie zapasowe umieszczone zostają na dyskach serwerowych oraz starsze dane na taśmach magnetycznych w celu obniżenia kosztów. Do przechowywanych danych należą:

- Dane finansowe klientów - pliki PDF, DOCX, pliki specyficzne dla programu Insert GT, bazy danych,
- Dane personalne klientów,
- Nagrania z monitoringu (miesiąc wstecz),
- Kopia zapasowa:
  - Kompresowana,
  - Codziennie różnicowa dla danych klientów (raz w tygodniu pełna),
  - Codziennie przyrostowa dla monitoringu,
  - Codziennie pełna kopia konfiguracji urządzeń,
- Dane zatrudnienia oraz księgowość firmy.

Wszystkie przechowywane dane mają charakter informacji wrażliwych, ponieważ firma głównie operuje na danych osobowych. Dane finansowe klientów maja charakter tajny, ze względu na niebezpieczeństwo wykorzystania tych informacji przez nieprzyjazną konkurencję.

Szacowany przyrost danych:

Tygodniowy przyrost danych oscyluje w okolicach 1 GB danych + kopia zapasowa około 500 MB. Kopia danych klientów z ostatniego roku trzymana jest na serwerze backupu. Kopie dalsze znajdują się na taśmach magnetycznych w archiwum - dodatkowo te, które tego wymagają są drukowane. Dane w archiwum przechowywane są przez 5 lat po tym okresie dane są przenoszone do osobnego archiwum.

2 Identyfikacja zagrożeń i analiza ryzyka

W niniejszym rozdziale zostanie przeprowadzony audyt bezpieczeństwa. Zostaną przedstawione potencjalne zagrożenia w systemie oraz zdefiniowana zostanie metoda oceny ryzyka.

2.1 Ocena ryzyka - metoda jakościowa

Do oceny ryzyka wykorzystano metodę jakościową OWASP Risk Rating Methodology. W zależności od wpływu oraz prawdopodobieństwa wystąpienia zagrożenia, określa się jakie ze sobą niesie ryzyko.

Tabela 1: Kryteria oceny jakościowej

Ryzyko				
Wpływ	Wysoki	Średnie	Wysokie	Krytyczne
	Średni	Niskie	Średnie	Wysokie
	Niski	Bardzo niskie	Niskie	Średnie
		Niskie	Średnie	Wysokie
	Prawdopodopieństwo			

2.2 Zagrożone zasoby

Każdy zasób należy chronić, ale nie wszystkie wymagają zabezpieczenia na jednolitym poziomie. W tabeli 2 znajduje się spis sprzętu oraz danych wraz z ich priorytetem ważności (1 — najważniejszy, 10 — najniższy), które zostaną brane pod uwagę podczas przeprowadzania audytu.

Tabela 2: Wykaz zasobów uwzględnianych w audycie

Lp.	**Zasób**	**Priorytet ważności**	**Opis**
Serwery:			
1	Kopie zapasowe	2	Dane potrzebne do odzyskania sprawności systemów
2	Dyski twarde	1	Pamięć trwała serwera
3	Baza danych	3	Przechowywanie wrażliwych danych klientów

4	Zasilanie	8	Utrzymanie pracy serwerów
Komputery pracowników:			
5	Dyski twarde	6	Pamięć trwała komputera
6	Kopie zapasowe	7	Dane potrzebne do odtworzenia systemu
7	Dane klientów	4	Dane osobowe oraz finansowe klientów
8	Zasilanie komputerów stacjonarnych	9	Utrzymanie pracy sprzętu
9	Zasilanie laptopów	10	Utrzymanie pracy sprzętu
10	Hasła użytkowników	5	Hasła systemowe użytkownikóa
Archiwum:			
11	Dokumenty papierowe	4	Dokumenty archiwalne klientów
12	Taśmy magnetyczne z kopiami zapasowymi	3	Dane potrzebne do odzyskania sprawności systemu
Inne:			
13	Rejestrator kamer	8	Nagrania z monitoringu
14	Sieć bezprzewodowa	6	Sieć połączona z siecią firmy
15	Switche sieciowe	6	Pośredniczą w przesyle danych przez sieć
16	Router	8	Umożliwia dostęp do Internetu
17	Telefony IP	6	Umożliwiają komunikację wewnątrz budynku
18	Bramka VoIP	5	Pośredniczy pomiędzy połączeniem telefonów IP
19	Zasilanie budynku	10	Zasilanie oświetlania, drzwi przesuwnych itp.
20	Dostępność do Internetu	10	Dostęp do Internetu od dostawcy

2.3 Zagrożenia systemu

W tym podrozdziale opisane zostaną potencjalne zagrożenia oraz w tabelach zostanie ocenione ryzyko jakie niosą ze sobą dane niebezpieczeństwa. Zagrożenia podzielono na trzy kategorie: zagrożenia naturalne, zagrożenia ludzkie oraz zagrożenia techniczne.

2.3.1 Zagrożenia naturalne

Zagrożenia naturalne związane są z lokalizacją przedsiębiorstwa, należą do nich:

- zanik prądu,
- upadek drzewa,
- pożar.

Wymienione zagrożenia mają wpływ na dostępność danych. W budynku nie ma systemu przeciwpożarowego, a więc podczas pożaru, wysoka temperatura może uszkodzić sprzęt. Również uszkodzenie sprzętu może nastąpić w czasie zaniku prądu. Zasilacze awaryjne (UPS) podczas braku prądu dostarczają energię elektryczną tylko do serwerów i pozostały sprzęt jest narażony na uszkodzenie. W tabeli 3 oceniono ryzyko związane z zagrożeniami naturalnymi.

Tabela 3: Zagrożenia naturalne

Podatność	**Zasoby**	**Prawdopodobieństwo**	**Wpływ**	**Ryzyko**
Zanik prądu	Serwer — zasilanie,	Niskie	Wysoki	Średnie
	Komputery pracowników — zasilanie	Średnie	Wysoki	Wysokie
	Bramka VoIP	Średnie	Niski	Niskie
	Telefon IP	Średnie	Niski	Niskie
	Rejestrator kamer	Średnie	Średni	Średnie
	Pozostałe zasoby	Niski	Niski	Bardzo niskie
Upadek drzewa	Wszystkie zasoby	Niski	Średni	Niskie
Pożar	Wszystkie zasoby	Niski	Wysoki	Średnie

2.3.2 Zagrożenia techniczne

System firmy narażony jest również na zagrożenia stricte związane z informatyka (aspektem technicznym). Niebezpieczeństwa ze strony technicznej wymieniono zostały w tabeli 4. Określono stopień ryzyka dla każdego istotnego zasobu systemu.

Tabela 4: Wykaz zagrożeń technicznych

Podatność	**Zasoby**	**Prawdopodobieństwo**	**Wpływ**	**Ryzyko**
Złamanie hasła administratora dowolnego komputera	Serwer — baza danych,	Wysokie	Wysoki	Krytyczne
	Komputery pracowników — dane klientów	Wysokie	Wysoki	Krytyczne
	Komputery pracowników — hasła użytkowników	Średnie	Wysoki	Wysokie
	Komputery pracowników — kopie zapasowe	Wysokie	Średni	Wysokie
	Bramka VoIP	Średnie	Średni	Średnie
	Telefon IP	Niskie	Średni	Niskie
	Rejestrator kamer	Niskie	Średni	Niskie
	Pozostałe zasoby	Niski	Niski	Bardzo niskie
Infekcja komputera wirusem typu ransomware	Serwer — kopie zapasowe	Wysokie	Wysoki	Krytyczne
	Serwer — dyski twarde	Wysokie	Wysoki	Krytyczne
	Serwer — baza danych	Wysokie	Wysoki	Krytyczne
	Komputery pracowników — dyski twarde	Wysokie	Średni	Wysokie
	Komputery pracowników — kopie zapasowe	Wysokie	Średni	Wysokie
	Komputery pracowników — dane klientów	Wysokie	Średni	Wysokie
	Rejestrator kamer	Wysokie	Niski	Średnie
	Pozostałe zasoby	Niskie	Niski	Bardzo niskie

Szkodliwe oprogramowanie	Serwer — kopie zapasowe	Średnie	Wysoki	Wysokie
	Serwer — dyski twarde	Średnie	Wysoki	Wysokie
	Serwer — baza danych	Średnie	Wysoki	Wysokie
	Komputery pracowników — dyski twarde	Wysokie	Średni	Wysokie
	Komputery pracowników — kopie zapasowe	Średnie	Średni	Średnie
	Komputery pracowników — dane klientów	Wysokie	Wysoki	Krytyczne
	Komputery pracowników — hasła użytkowników	Średnie	Wysoki	Wysokie
	Sieć bezprzewodowa	Niskie	Średni	Niskie
	Bramka VoIP	Średnie	Średni	Średnie
	Telefon IP	Średnie	Średni	Średnie
	Pozostałe zasoby	Niskie	Niski	Bardzo niskie
Zużycie sprzętu (dysk, zasilacz, inne podzespoły)	Serwer — dyski twarde	Wysokie	Wysoki	Krytyczne
	Serwer — kopie zapasowe	Wysokie	Wysoki	Krytyczne
	Serwer — dyski twarde	Wysokie	Wysoki	Krytyczne
	Serwer — zasilanie	Wysokie	Średni	Wysokie
	Komputery pracowników — dyski twarde	Niskie	Średni	Niskie
	Komputery pracowników — kopie zapasowe	Niskie	Średni	Niskie
	Pozostałe zasoby	Niskie	Niskie	Bardzo niskie

atak DDoS	Serwer — dyski twarde	niskie	wysoki	Krytyczne
	Serwer — baza danych	wysokie	wysoki	Krytyczne
	Komputery pracowników — dyski twarde	niskie	średni	Niskie
	Router	średnie	średnie	Średnie
	Pozostałe zasoby	niskie	niski	Bardzo niskie
atak hakerski (innego rodzaju)	Serwer — kopie zapasowe	wysokie	wysoki	Krytyczne
	Serwer — dyski twarde	wysokie	wysoki	Krytyczne
	Serwer — baza danych	wysokie	wysoki	Krytyczne
	Komputery pracowników — kopie zapasowe	wysokie	wysoki	Krytyczne
	Komputery pracowników — dyski twarde	wysokie	wysoki	Krytyczne
	Komputery pracowników — dane klientów	wysokie	wysoki	Krytyczne
	Router	średnie	średnie	Średnie
	Pozostałe zasoby	niskie	niski	Bardzo niskie

2.3.3 Zagrożenia ludzkie

Do zagrożeń ludzkich należą:

- kradzież sprzętu oraz dokumentów przez pracowników lub osoby spoza firmy,
- zainstalowanie zainfekowanego oprogramowania przez pracowników lub osoby spoza firmy,
- zniszczenie sprzętu przez pracowników lub osoby spoza firmy
- usunięcie danych przez pracowników lub osoby spoza firmy
- nieautoryzowana zmiana treści dokumentów przez pracowników lub osoby spoza firmy
- atak hakerski

Wyżej wymienione zagrożenia ludzkie wpływają na poufność, integralność oraz na dostępność danych. Do budynku łatwo można się wkraść, ponieważ nie ma wystarczającej ilości kamer, aby odpowiednio monitorować cały obiekt. Dodatkowo, system monitoringu nie ma awaryjnego zasilania i w chwili zaniku prądu jest bezużyteczny. Również brakuje alamów przy drzwiach oraz oknach. Pracownicy mogą dostać się do pomieszczeń za pomocą zwykłych kluczy. Taka sytuacja powoduje, że osoba używająca np. wytrychu jest wstanie w krótkim czasie dostać się do jakiekolwiek pomieszczenia. Brak oprogramowania służącego do blokowania stron internetowych umożliwia wejście na takie strony i nieświadome zawirusowanie sprzętu. Na serwerach nie ma zainstalowanych dodatkowych programów związanych z bezpieczeństwem, przez co sprzęt narażony jest na ataki hakerskie. Pracownicy mogą skopiować dokumenty przedsiębiorstwa, ponieważ porty USB nie są zabezpieczone. Brak też zabezpieczeń w komunikacji między komputerami i między komputerem a drukarką. Istnieje więc ryzyko nie tylko przejęcia pliku, ale również jego zmodyfikowanie przez nieautoryzowaną osobę. W tabeli 5. oceniono ryzyko związane z zagrożeniami ludzkimi.

Tabela 5: Wykaz zagrożeń ludzkich

Podatność	**Zasoby**	**Prawdopodobieństwo**	**Wpływ**	**Ryzyko**
Kradzież sprzętu oraz dokumentów przez pracowników lub osoby spoza firmy	Serwer — kopie zapasowe	wysoki	wysoki	krytyczne
	Serwer — dyski twarde	średnie	wysoki	krytyczne
	Serwer — baza danych	średnie	wysoki	krytyczne
	Komputery pracowników — kopie zapasowe	średnie	wysoki	wysokie
	Komputery pracowników — dyski twarde	średnie	wysoki	wysokie
	Archiwum — dokumenty papierowe	średnie	wysoki	wysokie
	Archiwum — taśmy magnetyczne z kopiami zapasowymi	średnie	wysoki	wysokie
	Pozostałe	niskie	średni	niskie
zainstalowanie zainfekowanego oprogramowania przez pracowników lub osoby spoza firmy	Komputery pracowników — dyski twarde	wysokie	wysoki	krytyczne
	Komputery pracowników — dane klientów	wysokie	wysoki	krytyczne
	Komputery pracowników — kopie zapasowe	wysokie	wysoki	krytyczne
	Rejestrator kamer	średnie	średni	średnie
	Router	średnie	wysoki	wysokie
	Dostęp do Internetu	średnie	wysoki	wysokie
	Pozostałe	niskie	niski	bardzo niskie

Zniszczenie sprzętu przez pracowników lub osoby spoza firmy	Serwer — kopie zapasowe	niskie	wysoki	średnie
	Serwer — dyski twarde	niskie	wysoki	średnie
	Serwer — baza danych	niskie	wysoki	średnie
	Komputery pracowników — dyski twarde	średnie	wysoki	wysokie
	Komputery pracowników — kopie zapasowe	średnie	wysoki	wysokie
	Komputery pracowników — dane klientów	średnie	wysoki	wysokie
	Archiwum — taśmy magnetyczne z kopiami zapasowymi	niskie	wysoki	średnie
	Pozostałe	niskie	średni	niskie
usunięcie danych przez pracowników lub osoby spoza firmy	Serwer — kopie zapasowe	średnie	wysoki	wysokie
	Serwer — baza danych	średnie	wysoki	wysokie
	Komputery pracowników — kopie zapasowe	średnie	średni	średnie
	Komputery pracowników — dane pracowników	średnie	wysoki	wysokie
	Komputery pracowników — dyski twarde	średnie	wysoki	wysokie
	Pozostałe zasoby	niskie	niskie	bardzo niskie

Nieautoryzowana zmiana treści dokumentów przez pracowników lub osoby spoza firmy	Serwer — kopie zapasowe	niskie	średni	niskie
	Serwer — baza danych	średnie	wysoki	wysokie
	Komputery pracowników — kopie zapasowe	niskie	średni	niskie
	Komputery pracowników — dane klientów	średnie	wysoki	wysokie
	Archiwum — dokumenty papierowe	niskie	średni	niskie
	Archiwum — taśmy magnetyczne z kopiami zapasowymi	niskie	średni	niskie
	Pozostałe zasoby	niskie	niski	bardzo niskie

3 Proponowane zmiany minimalizujące ryzyko wystąpienia zagrożeń

W poniższym rozdziale zostaną zaprezentowane propozycje, które zmniejszą ryzyko wystąpienia zagrożeń:

- w celu zmniejszenia prawdopodobieństwa wystąpienia pożaru, czy też zmniejszenia skutków wymienionego zagrożenia, należy rozważyć instalację systemu przeciwpożarowego w budynku, szczególnie w serwerowni oraz umieścić w pomieszczeniach gaśnice
- aby, zmniejszyć negatywne skutki zaniku prądu, zaleca się wymianę komputerów stacjonarnych na laptopy oraz dołożyć dodatkowy zasilacz awaryjny (UPS), który będzie obsługiwał kamery wraz z rejestratorem
- zamontowanie klimatyzacji w archiwum, w celu przedłużenia czasu przechowywania danych na nośnikach
- zamontowanie większej ilości kamer wokół budynku
- zastąpienie drzwi wejściowych, drzwi do serwera oraz drzwi do archiwum, na drzwi otwierane za pomocą karty magnetycznej
- wprowadzając szkolenia dotyczące bezpiecznego używania sprzętu oraz sieci internetowej, zmniejsza się prawdopodobieństwo m.in. wystąpienia przypadkowego zainfekowania komputera przez pracownika
- w celu zmniejszenia złamania haseł do komputerów, należy wymusić używanie haseł o minimalnej długości 8 znaków, zawierających minimum jedną cyfrę, jedną wielką literę i jedną cyfrę oraz wymusić zmianę haseł co 30 dni
- zainstalowanie zaawansowanego pakietu zabezpieczającego komputer Avast Premier
- regularne aktualizowanie oprogramowania oraz skanowanie urządzeń programem antywirusowym
- wprowadzenie okresowych audytów bezpieczeństwa
- szyfrowanie przesyłanych danych między urządzeniami podłączonymi do sieci internegowej
- blokowanie nieznanych urządzeń podłączanych do komputera
- oddzielenie sieci przewodowej od bezprzewodowej za pomocą dwóch osobnych połączeń między dostawcą Internetu a przedsiębiorstwem
- zamontowanie odbiorników GPS w urządzeniach w celu odnalezienia ukradzionego sprzętu

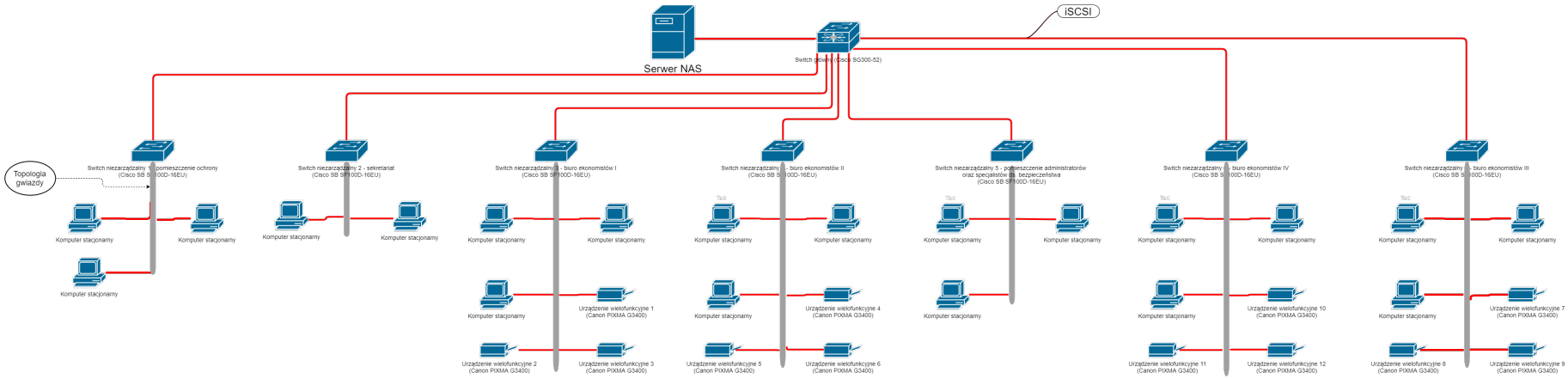
- oznakowanie sprzętu specjalną farbą w celu łatwiejszej weryfikacji ukradzionego sprzętu
- dokupienie zapasowego sprzętu w celu szybszego powrotu do funkcjonowania przedsiębiorstwa
- monitorowanie ruchu sieciowego
- szyfrowanie dysków w serwerach i komputerach pracowników

4 System przechowywania danych

Rozdział ten przedstawia propozycję systemu przechowywania danych. Struktura sieci informatycznej jest rozbudowana, zatem aby scentralizować dostęp do danych zastosowano technologię NAS.

4.1 Struktura NAS

Dostęp do serwera NAS nie wymagają telefony IP oraz bramka VoIP, zatem nie zostały uwzględnione w strukturze. Schemat systemu NAS znajduje się na rysunku 5. Połączenia pomiędzy stacjami roboczymi poprowadzone są poprzez iSCSI (wykorzystując sieć przewodową).



Rys. 5: Schemat struktury NAS

4.2 Serwer

Serwer główny ze względu na potrzebę niezawodności pracy posiada macierz dyskową RAID 4 z 3 dyskami HDD WD Red 2TB. W przypadku awarii dowolnego dysku istnieje możliwość odtworzenia utraconych danych. Jest to wolniejsze rozwiązanie niż powiedzmy RAID 5, ale zapewnia większe bezpieczeństwo w przypadku uszkodzenia. Wykorzystując daną macierz dyskową posiadamy 4TB pojemności dyskowej, wg podanych informacji od zleceniodawców taki rozmiar pamięci powinien wystarczyć na przechowywanie danych przez 50 lat (jest to okres przez jaki należy przechowywać dane księgowe).

Serwer zapasowy posiada kompletną kopię macierzy dyskowej z serwera głównego zapewniając redundancję w przypadku całkowitej awarii sprzętu. W ten sposób zabezpieczamy w znacznym stopniu dane przed utraceniem.

Na serwerze w środowisku wirtualnym uruchomiony jest system FreeNAS odpowiedzialny za zarządzanie przechowywaniem plików. W systemie FreeNAS uruchomione są usługi odpowiedzialne za replikację danych oraz tworzenie kopii zapasowych. Pełna kopia zapasowa będzie wykonywana w każdy poniedziałek, natomiast kopia przyrostowa będzie wykonywana w pozostałe dni tygodnia. Każda kopia zapasowa będzie szyfrowana algorytmem AES.

Dodatkowo kopie zapasowe z okresu powyżej roku przechowywane są na taśmach magnetycznych w pomieszczeniu archiwum.

4.3 Komputery pracowników

Komputery pracowników ze względu na nie zbyt wysoką szkodliwość utraty danych (pod warunkiem przenoszenia danych systematycznie do pamięci serwera - NAS) nie wymagają szczególnych zabezpieczeń. Wykorzystano dwa rodzaje dysków: HDD WD Black 500GB dla plików oraz SSD Samsung 850 Pro 120GB dla wybranych programów oraz systemu operacyjnego. W przypadku braku dwóch slotów dyskowych drugi dysk (HDD) zastępuje napęd optyczny. Magistralą użytą w komputerach jest SATAIII ze względu na parametry techniczne komputerów (brak magistrali NVIe).