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.

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

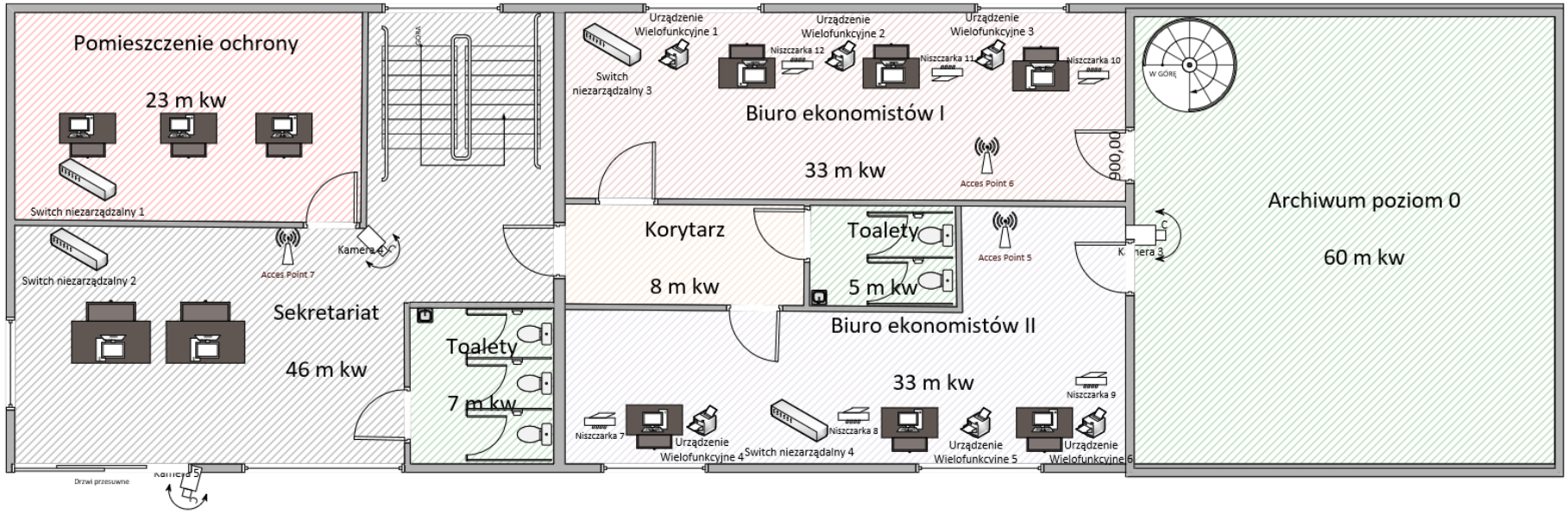
Firma jest biurem rachunkowym specjalizującym się w doradztwie finansowym, prowadzaniu księgowości dla przedsiębiorstw oraz przygotowywaniu analizy finansowej rynku. Przedsiębiorstwo zatrudnia 42 osoby, które tworzą cztery działy: dział ekonomistów, dział sprzedaży, dział IT i dział obsługi.

1.2 Opis budynku

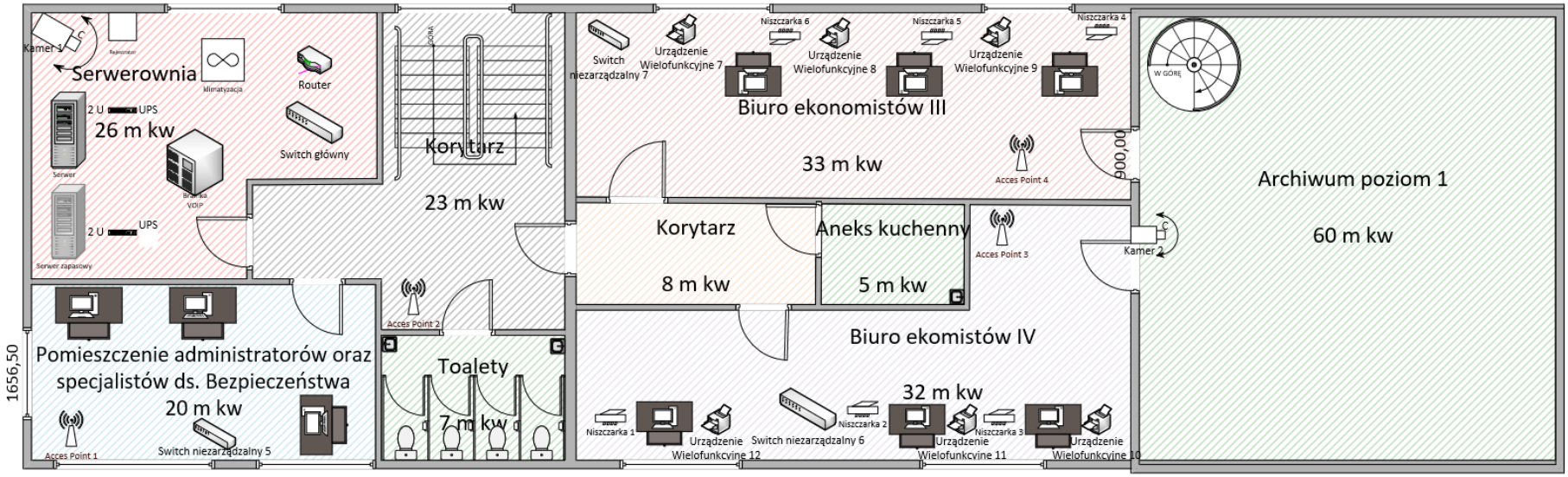
Dwupiętrowy budynek firmy zlokalizowany jest na obrzeżach dużego miasta. W okolicy jest pomijalnie niskie ryzyko wystąpienia klęsk żywiołowych. Budynek otaczają stare drzewa, których nie można wyciąć, ponieważ objęte są ochroną gatunkową. Do przedsiębiorstwa doprowadzona jest sieć telefoniczna oraz internetowa.

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

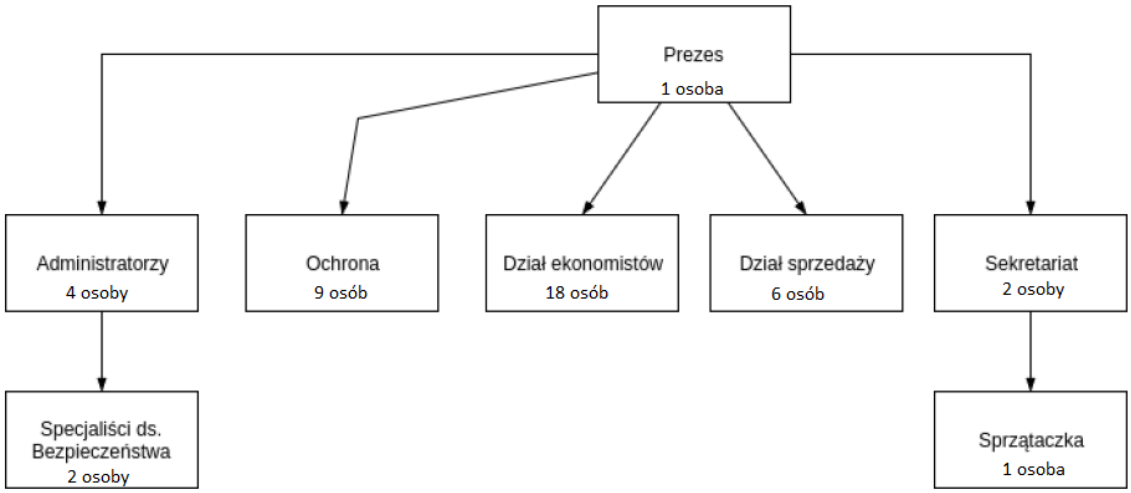
1.3 Organizacja pracy

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:

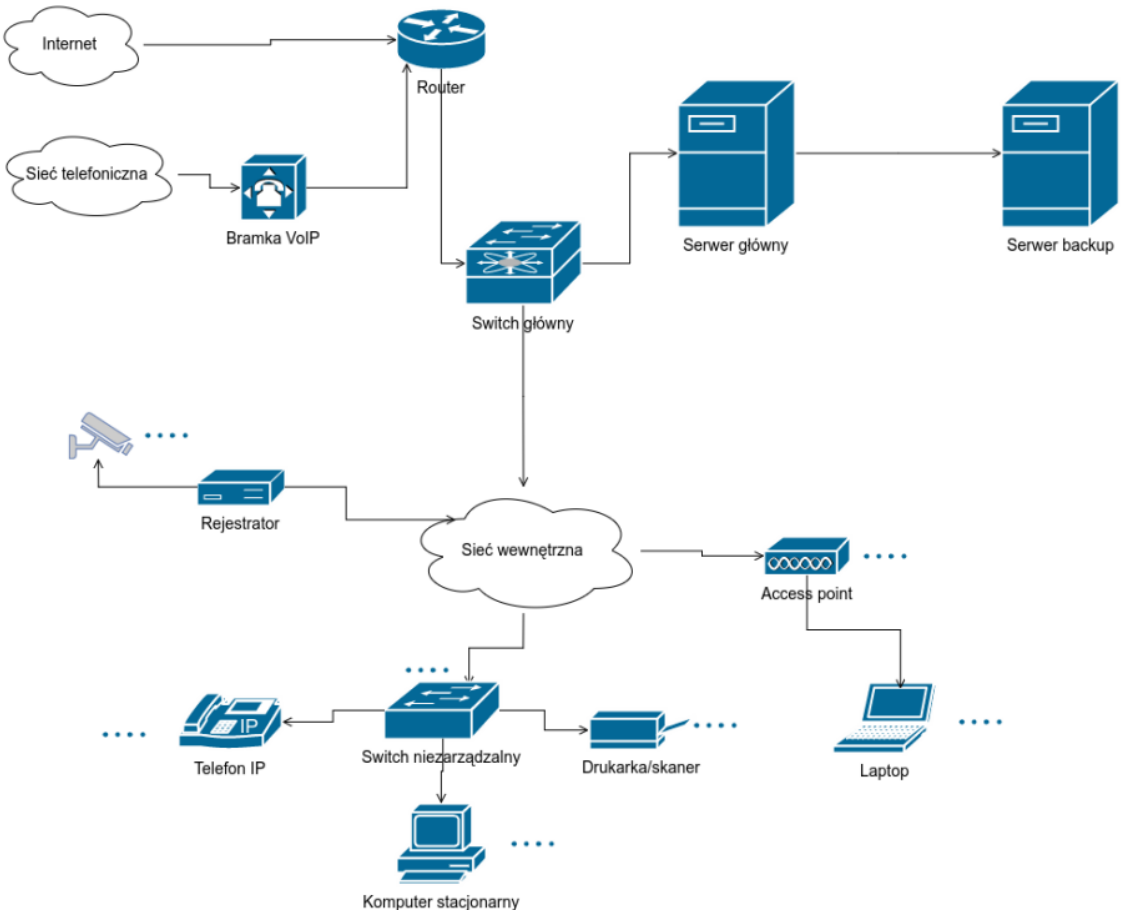
- urządzenie wielofunkcyjne Canon PIXMA G3400 (12 sztuk),
- niszczarka ProfiOffice PIRANHA EC 7 CC (12 sztuk),
- komputer stacjonarny (18 sztuk):
  - procesor Intel i5,
  - pamięć 8 GB RAM DDR3,
  - dysk 1 TB HDD,
  - myszka, klawiatura, monitor 24",
- laptop DELL Inspiron 5567 (dział IT 6 sztuk),
- 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

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,

1.6 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: Ocena ryzyka

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

2.2 Potencjalne zagrożenia

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 (wpływ na dostępność 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.
Wpływ - średni, prawdopodobieństwo - niskie, ryzyko - niskie.

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.

Skutki mogą być poważne. Włamywacz nie tylko może ukraść sprzęt/dane (zagrożenie zasad poufności danych), ale także może zainstalować oprogramowanie szpiegujące lub zmodyfikować istniejące dane (wpływ na zasady integralności danych).
Wpływ - wysoki, prawdopodobieństwo - średnie, ryzyko - wysokie.

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 (naruszenie zasad integralności oraz poufności).
Wpływ - wysoki, prawdopodobieństwo - średnie, ryzyko - wysokie.

Hackerzy mają ułatwione zadanie związane z dostaniem się na serwery dlatego, że w serwerach nie jest używane dodatkowe oprogramowanie związane z bezpieczeństwem (złamanie zasady poufności oraz wysokie zagrożenie integralności danych). Nie ma też sprzętowej zapory ogniowej, która filtrowałaby cały ruch sieciowy.
Wpływ - wysoki, prawdopodobieństwo - wysokie, ryzyko - krytyczne.

Firma nie jest odpowiednio przygotowana na spadki napięcia lub zanik prądu, ponieważ w czasie awarii zasilania wszystkie komputery, kamery razem z rejestratorem obrazu i inne urządzenia elektryczne wyłączą się. Nagłe wyłączenie się komputerów może spowodować utratę ważnych danych lub też uszkodzenie komponentów w komputerze (wysoki stopnień naruszenia zasad dostępności oraz integralności). Wyłączenie się kamer utrudnia ochronę budynku. Zasilacze awaryjne (UPS) dostarczają energię elektryczną tylko do serwerów.
Wpływ - wysoki, prawdopodobieństwo - średnie, ryzyko - wysokie.

Brak wystarczającej ilości kamer, aby odpowiednio monitorować budynek z zewnątrz i wewnątrz. Kamery przy wejściu do budynku i w sekretariacie na parterze mają zbyt dużą powierzchnię do monitorowania, co powoduje istnienie martwych pól przez długi czas. Wówczas poruszając się poza widocznością kamery można włamać się (skutki zostały opisane wcześniej).

Monitory obrócone w stronę okna umożliwiają podejrzenie co dana osoba wykonuje na komputerze, zatem naruszona zostaje poufności przeglądanych materiałów.
Wpływ - średni, prawdopodobieństwo - niskie, ryzyko - niskie.

Brak polityki bezpieczeństwa powoduje sytuację, w której użytkownicy mogą używać prostych haseł, czy też przez długi okres czasu nie zmieniać ich. Uruchomiony odpowiedni program może złamać takie hasła niezależnie

od skomplikowania hasła, również hasło może być poznane w stosunkowo krótkim czasie, czy będzie trywialne. Uzyskanie dostępu do sytemu przez nieupoważnione osoby spowoduje naruszenie zasady poufności. Osoba taka może również zmienić hasło użytkownika, co ograniczy dostępność do zasobów, można również zmodyfikować dane naruszając integralność.
Wpływ - wysoki, prawdopodobieństwo - wysokie, ryzyko - krytyczne.

Niezabezpieczone porty USB umożliwiają użytkownikowi nie tylko kopiowanie danych z firmy, ale również zainfekowanie komputera, czy też jego uszkodzenie przy użyciu np. USB Killer (zagrożenie dla poufności danych, dostępności oraz integralności).
Wpływ - wysoki, prawdopodobieństwo - wysokie, ryzyko - krytyczne.

Nieużywanie programów do blokowania instalacji programów ułatwia użytkownikowi wgranie dowolnego oprogramowania. Bez blokowania dostępu do wybranych stron internetowych, użytkownicy mogą wchodzić na strony zainfekowane (zgrożenie dla poufności danych i integralności).
Wpływ - wysoki, prawdopodobieństwo - niskie, ryzyko - średnie.

Bezpieczeństwo poczty elektronicznej jest zapewnione przez używanie odpowiedniego oprogramowania. Natomiast, komunikacja w celu wysłania pliku między komputerami lub między komputerem a drukarką nie jest zabezpieczona. Istnieje więc ryzyko zmodyfikowania pliku, bądź też jego przejęcia przez nieautoryzowaną osobę (zagrożenie dla poufności danych i integralności).
Wpływ - wysoki, prawdopodobieństwo - niskie, ryzyko - średnie.

Kolejnym zagrożeniem jest topologia sieci internetowej, a konkretniej połączenie poprzez sieć bezprzewodową. Istnieje możliwość wykorzystania sieci otwartej WiFi do przedostania się do innych podsieci, a nawet w skrajnym przypadku do serwerów (naruszenie poufności oraz integralności danych). Również niebezpieczeństwem związanym z siecią jest brak alternatywnego połączenia z Internetem (brak zapewnienia dostępności).
Wpływ - wysoki, prawdopodobieństwo - średnie, ryzyko - wysokie.