Piotrków Tryb. 13.12.2013 r.

Urząd Miasta
Piotrkowa Trybunalskiego
Referat Informatyki
97-300 Piotrków Tryb.
Pasaż Rudowskiego 10

DBM.015.9.2013

Pani Renata Karbowniczek

Dyrektor BOMiNO

Dotyczy: Odpowiedzi na pismo DBM.015.9.2013 w sprawie wytycznych w zakresie warunków funkcjonowania Biura Obsługi Mieszkańców w budynku przy ul. Szkolnej.

WYTYCZNE DO PROJEKTU SIECI TELEINFORMATYCZNEJ I MIEJSC PRZETWARZANIA DANYCH OSOBOWYCH

Integralną częścią struktury Biura Obsługi Mieszkańców jest szeroko rozumiana sieć teleinformatyczna. W jej skład wchodzi sieć telefoniczna, sieć komputerowa oraz wszelkie elementy związane z obsługą oraz zabezpieczeniem obu sieci. Do elementów takich zaliczyć możemy m.in. elementy aktywne i pasywne sieci, jak również strukturę zasilania wraz z mechanizmami zasilania awaryjnego.

Każde stanowisko pracy powinno być wyposażone w:

1. Zestaw komputerowy.
2. Odpowiednie urządzenia peryferyjne przewidziane dla poszczególnych stanowisk.
3. Gniazdo sieci komputerowej oraz gniazdo teleinformatyczne (RJ-45 - umożliwiające naprzemienne podłączanie telefonu i urządzenia sieci komputerowej) oraz możliwość podłączenia sieciowego urządzenie peryferyjnego (preferowana ilość gniazd – 4 szt.).
4. Przyłącze elektryczne z zabezpieczeniem przepięciowym (filtrowanie na poziomie zasilacza awaryjnego) wyposażone w min. 3 gniazda sieciowe z zerowaniem.

Na potrzeby BOM przewiduje się wykonanie sieci komputerowej w technologii Ethernet 1 Gb/s (Gigabit Ethernet) opartej na przełącznikach sieciowych o prędkości 1 Gb/s.

Okablowanie strukturalne sieci komputerowej musi spełniać wymagania technologii 1 Gb/s.

Zalecane jest kompleksowe podejście do okablowania na etapie projektu i wykonania.

Należy wydzielić odrębne pomieszczenie (lokalny punkt dystrybucyjny „serwerownia”), który powinien być w miarę odizolowany od ciągów komunikacyjnych i ze względu na czynności związane z obsługą tworzenia kopii zapasowych był możliwie blisko stanowisk referatu komunikacji. Punkt ten zostanie połączony łączami światłowodowymi z punktem dystrybucyjnym znajdującym się na w pokoju 29 w budynku Szkolna 28 II piętro.

Cechy lokalnego punktu dystrybucyjnego dla BOM:

1. Lokalizacja punktu w zamkniętym pomieszczeniu, zabezpieczonym fizycznie, ograniczona maksymalnym zasięgiem okablowania poziomego (90 m).
2. Instalacja elektronicznego systemu kontroli dostępu, wykrywania włamań oraz wykrywania pożaru.
3. Wydzielona sieć energetyczna do zasilania sprzętu komputerowego i serwerowni z odpowiednimi zabezpieczeniami przeciwprzepięciowymi i przeciwporażeniowymi.

4. Urządzenia do zachowania odpowiednich warunków fizycznych, temperatura - ok. 20°C - klimatyzacja, wymuszony obieg powietrza i wilgotność - 30-50%.
5. Drzwi otwierane na zewnątrz o szerokości min. 0,9 m.
6. Przepusty w ścianach na wyprowadzenie odpowiedniej ilości okablowania wg stosownych projektów sieci - rury bądź rękawy, przelot z zapasem zapewniającym możliwość instalacji dodatkowego okablowania w przyszłości.
7. Odpowiedniej wielkości szafa dystrybucyjna zapewniająca pomieszczenie urządzeń aktywnych i pasywnych sieci komputerowej i telefonicznej a także doprowadzenie przebiegów kablowych, z możliwością umieszczenia dodatkowych urządzeń w przyszłości, oraz zapewnieniem swobodnego dostępu i odpowiedniej wentylacji. Wskazany montaż jest montaż dwóch szaf w celu fizycznego odseparowania sieci LAN Urzędu Miasta i sieci systemu Pojazd - Kierowca.
8. Odpowiednia powierzchnia punktu dystrybucyjnego, pomieszczenia serwerowni min. 12 m^2.

Celem zapewnienia ciągłej pracy komputerowego systemu wspomagającego pracę BOM, sieć należy wyposażyć w układ podtrzymywania napięcia z automatycznym przełączaniem w przypadku awarii zasilania, z czasem podtrzymania zasilania umożliwiającym usunięcie podstawowych usterek.
Wymagania ochrony fizycznej powinny być dostosowane do wymogów ustawy o ochronie danych osobowych, a w szczególności:

1. Pomieszczenia, w których zlokalizowane są stacje robocze przeznaczone do pracy w rozwiązaniu ADSxP, wyposażone m. in. w czytniki mikroprocesorowych kart kryptograficznych i drukarki oraz pomieszczenia, gdzie przetwarzane i przechowywane są informacje pobrane z bazy danych CEPIK, nie mogą być pomieszczeniami przechodnimi - rozumiemy przez to taką sytuację gdzie pomieszczenia służące do przetwarzania danych osobowych nie mogą służyć, jako ciąg komunikacyjny dla interesantów ani pracowników innych komórek organizacyjnych (obszar zadań wykonywanych przez referat komunikacji).
2. Kontrolę dostępu do pomieszczeń zapewnia się poprzez automatyczne lub manualne systemy kontroli dostępu (urządzenia automatycznej kontroli dostępu winny być nadzorowane całodobowo przez służbę ochrony. W przypadku braku systemu automatycznego, kontrola dostępu do pomieszczeń powinna być realizowana metodami organizacyjno-proceduralnymi przez wyznaczone osoby) - mechanizm kontroli dostępu musi dać możliwość zidentyfikowania osoby odpowiedzialnej za pomieszczenie po godzinach pracy.

   Alternatywne sposoby realizacji:

   1) automatyczny system kontroli dostępu (czytniki kart magnetycznych, wprowadzenie unikalnego kodu dostępu na manipulatorze itp.) z rejestracją wejść i wyjść,

   2) organizacja gospodarki kluczami: rejestrowanie danych osoby, która pobiera lub zdaje klucz oraz godziny pobrania/zdania klucza na podstawie listy osób upoważnionych, zdeponowanej u pracownika ochrony/portiera. Klucze powinny być przechowywane w zaplombowanych woreczkach/pojemnikach aby uniemożliwić pracownikowi ochrony niekontrolowany dostęp do chronionych pomieszczeń,

   3) w przypadku braku pracownika ochrony i zamykania pomieszczeń wydziału komunikacji i budynku po godzinach pracy, należy opracować procedurę otwierania i zamykania budynku i pomieszczeń, w której powinny być wymienione osoby upoważnione do zabierania ze sobą kluczy do pomieszczeń
   oraz podane numery telefonów pod którymi te osoby są natychmiast osiągalne, w przypadku wystąpienia zagrożenia W tych pomieszczeniach (np. włamanie lub pożar).
3. Pomieszczenia powinny być zlokalizowane w miejscach uniemożliwiających ich zatopienie lub zalanie,
4. Drzwi do pomieszczeń powinny być zabezpieczone drzwiami z dwoma zamkami, w tym jednym klasy C - chodzi tu o utrudnienie możliwości podrobienia klucza

   Alternatywne sposoby realizacji:

   1) zabezpieczenie całego obszaru danych osobowych jednymi drzwiami do całego obszaru, posiadającymi 2 zamki, w tym jeden klasy C (jeśli jest taka możliwość),

2) zabezpieczenie oddzielnie każdych drzwi do pomieszczeń drzwiami z dwoma zamkami, w tym jednym klasy C.

5. Otwory okienne pomieszczeń zlokalizowanych poniżej pierwszego piętra winny być okratowane lub zabezpieczone w inny równoważny sposób,

   Alternatywne sposoby realizacji:

   1) zamontowanie krat w oknach,

   2) zamontowanie okien antywłamaniowych,

   3) zabezpieczenie szyb W oknach folią wzmacniająca, przy jednoczesnym zastosowaniu instalacji alarmowej w pomieszczeniu, ze sprawnymi czujkami ruchu skierowanymi na otwory okienne. System alarmowy powinien być wyposażony w powiadamianie o naruszeniu bezpieczeństwa chronionego pomieszczenia służby/firny ochroniarskiej, która powinna W czasie nie dłuższym niż np. 5 minut pojawić się na miejscu zdarzenia (trzeba to sprecyzować w umowie z firmą).

6. Serwer, urządzenia aktywne sieci oraz stanowiska, na których są przetwarzane dane osobowe muszą być zabezpieczone przed utratą danych na skutek zaniku napięcia zasilającego,

7. Zamontowanie instalacji alarmowej pożarowej wyposażonej w czujki dymu lub temperatury,

   Alternatywne sposoby realizacji:

   1) montaż wydzielonej instalacji alarmowej pożarowej,

   2) montaż instalacji alarmowej pożarowej zespolonej z instalacją alarmowa antywłamaniową,

   3) montaż autonomicznych czujek dymu lub temperatury zasilanych bateryjnie z sygnalizacja dźwiękową.