ENEA Centrum sp. z o.o.
Ul. Górecka 1
60-201 Poznań

NIP 777 00 02 843
REGON 630770227
www.enea.pl

Poznań, 28.04.2021r.

ODPOWIEDZI ZAMAWIAJĄCEGO NA PYTANIA WYKONAWCÓW VI

Sygnatura postępowania: 1400/DW00/ZU/KZ/2021/0000012428
Sygnatura pisma: DL/LZ/NB/2021/780

Dotyczy postępowania pn.:

Kompleksowa obsługa wydruku masowego dokumentacji wychodzącej dla GK ENEA

Działając na podstawie pkt. 1.9 Warunków Zamówienia (dalej: WZ) Zamawiający udziela wyjaśnień dokumentacji przedmiotowego postępowania:

<table>
<tr><th>Lp.</th><th>Treść pytania wraz z odpowiedzią</th></tr>
<tr><td>1.</td><td>
Dotyczy:
<table>
<tr><td>3.</td><td>Dotyczy:
Czy Zamawiający nadal oczekuje zwrotnie projektów aplikacji w oprogramowaniu GMC (Quadient Inspire) czy jednak w oprogramowaniu z którego faktycznie będzie generowana korespondencja po stronie Wykonawcy?
Zapisy umowne udostępnione w dniu 20.04.2021 nadal wskazują, iż po zakończeniu Umowy Wykonawca przekaże Zamawiającemu wszystkie projekty przygotowane w oprogramowaniu GMC.
Cyt.
d) Wykonawca zobowiązany jest do przygotowania dokumentu funkcjonalnego opisującego zasady wdrożenia i realizacji usługi wydruku masowego w rozbiciu na poszczególne produkty wymienione w ust. 2. Zasady będą opisywały m.in. sposób wydruku (jednostronny, dwustronny), rodzaj Dokumentów wysyłanych listem zwykłym lub poleconym. Za bieżącą aktualizację Dokumentu funkcjonalnego odpowiedzialni są Koordynatorzy Umowy. Po str. 5
zakończeniu Umowy Wykonawca przekaże Zamawiającemu wszystkie przygotowane dla Zamawiającego w toku realizacji Umowy projekty Dokumentów w oprogramowaniu GMC.
Odpowiedź:
Tak, Zamawiający oczekuje zwrotu projektów w oprogramowaniu GMC.</td></tr>
</table>

W związku z akceptacją Zamawiającego, w zakresie wykonania po stronie Wykonawcy szablonów w innym oprogramowaniu niż GMC (odpowiedź nr 31 z dnia 20.04) oraz nie odrzuceniu możliwości przygotowania projektów na podstawie specyfikacji (odpowiedź nr 2 z dnia 22.04), Wykonawca zwraca się z prośbą o umożliwienie zwrotu projektów do Zamawiającego (po zakończeniu umowy) w oprogramowaniu, w którym zostaną one wykonane przez Wykonawcę tj. innym niż GMC (do projektów dołączona zostanie aktualizacja specyfikacji).
Nie ma możliwości aby wdrożenie przeprowadzić w oprogramowaniu X natomiast zwrócić do Zamawiającego projekty zgodne z oprogramowaniem Y.

Odpowiedź :
Zamawiający wymaga zwrócenia projektów w programie GMC, ponieważ obecne projekty są utworzone w tym oprogramowaniu i zawierają szereg zasad wydruku wszystkich szablonów dokumentów.
Każdorazowe wdrażanie wydruku dokumentów Zamawiającego od podstaw i tworzenie projektów w różnych oprogramowaniach co 3 lata wiąże się z wysokim ryzykiem błędnego wydruku oraz dużymi nakładami czasu pracy i kosztów. Do Wykonawcy należy decyzja biznesowa jakie oprogramowanie zastosuje do budowy projektów, jednak w przypadku przekazania przez Zamawiającego projektów w GMC, Wykonawca zobowiązany jest je odczytać i zastosować zapisane w nich zasady wydruku.
Zamawiający oczekuje zwrócenia projektów w oprogramowaniu GMC.</td></tr>
<tr><td>2.</td><td>Zamawiający określa w szczegółowym opisie przedmiotu zamówienia, ze wersja I i II wydruku może być stosowana w tym samym czasie:
„Zamawiający zastrzega prawo do wydruku dokumentów w dowolnej wersji. Wybrana wersja wydruku może zostać zmieniona przez Zamawiającego w dowolnym momencie. Jest możliwość, że w tym samym</td></tr>
</table>

ENEA Centrum sp. z o.o.
Ul. Górecka 1
60-201 Poznań

NIP 777 00 02 843
REGON 630770227
www.enea.pl

	czasie będą stosowane różne wersje wydruku, np. dokumenty rozliczeniowe będą drukowane według Wersji II, a pisma wysyłane na podstawie przesłanej bazy według Wersji I." Czy powyższe oznacza dla Wykonawcy wdrożenie obu wariantów dla wszystkich dokumentów? Ile czasu będzie miał Wykonawca na wprowadzenie zmiany technologii produkcji od momentu zgłoszenia przez Zamawiającego?
	Odpowiedź: Obecnie stosowany jest tylko jeden wariant wydruku – Wersja I, czyli w kolorze. W przypadku konieczności wdrożenia wydruku w Wersji II, Zamawiający i Wykonawca wspólnie ustalą termin wdrożenia zmiany.
3.	Część II – Wersja I – materiały informacyjne Czy Zamawiający wyraża zgodę na nadruk adresu zwrotu, adresu strony internetowej oraz opłaty pocztowej w kolorze czarnym? (Logotyp zostanie wydrukowany w kolorze)
	Odpowiedź: Zamawiający dopuszcza nadruk adresu zwrotu, adresu strony internetowej oraz opłaty pocztowej w kolorze czarnym, jednak kolorem preferowanym jest kolor szary.
4.	Przekazywanie do nadawania - Zamawiający oczekuje od Wykonawcy: „e) drukowania pocztowej książki nadawczej oraz opracowywania niezbędnych dokumentów zgodnych z zaakceptowanymi przez Zamawiającego wymaganiami operatora pocztowego, w przypadku nadawania dokumentów do wysyłki listami poleconymi, ekonomicznymi lub listami poleconymi za potwierdzeniem odbioru. Zeskanowane, potwierdzone przez operatora pocztowego, dokumenty dostępne będą na serwerze SFTP. Skany dokumentów będą przekazywane w formacie PDF raz w tygodniu za tydzień poprzedni. Opis – tytuł każdego dokumentu będzie umożliwiał identyfikację i sprawne odszukanie plików przez pracowników Zamawiającego w związku z potrzebami Zamawiającego (w tytule dokumentu umieszczona zostanie data nadania do operatora pocztowego);" Jednocześnie wskazuje obowiązek wdrożenia aplikacji operatora pocztowego Elektroniczny Nadawca. Czy Zamawiający podtrzymuje konieczność wydruku papierowych książek nadawczych?
	Odpowiedź: Wykonawca nie będzie musiał drukować papierowych książek nadawczych w przypadku pełnego wdrożenia Elektronicznego Nadawcy i potwierdzenia przez operatora pocztowego braku konieczności wydruku wersji papierowej.
5.	Formularz oferty 2. Część I – kolor– okres 36 miesięcy. b) Wydruk materiałów marketingowych/ pozostałe usługi 3. Część I – czerń– okres 36 miesięcy. c) Wydruk materiałów marketingowych/ pozostałe usługi Wykonawca wnioskuje o wskazanie min. ilości do jednorazowego zamówienia materiałów wskazanych w powyższych punktach w formularzu oferty.
	Odpowiedź: Zamawiający nie wyraża zgody na wskazanie minimalnych wolumenów. Każde zamówienie musi być dostosowane do potrzeb Zamawiającego. Na podstawie danych historycznych Zamawiający informuje, że dotychczasowe zamówienia były zawsze większe niż 1000 szt.
6.	Wymaganie dotyczące posiadania dwóch własnych niezależnych serwerowni, z wyłączeniem usługi kolokacji, jest wymaganiem, z którym nie spotkaliśmy się w trakcie prowadzenia naszej działalności. Takie podejście jest nietypowe i w oczywisty sposób preferuje firmy, które mają kilka lokalizacji oraz wiąże się z dodatkowymi kosztami po stronie Wykonawcy. Ponawiamy zapytanie o możliwość zastosowania usługi kolokacji. W razie odmowy prosimy o uzasadnienie czym ten wymóg jest spowodowany.
	Odpowiedź: Zamawiający wyraża zgodę na korzystanie z usługi kolokacji. W załączonym dokumencie znajdują się minimalne wymagania, które muszą zostać spełnione. Na etapie wdrożenia Wykonawca zobowiązany jest potwierdzić spełnienie wszystkich wymagań ze służbami IT Zamawiającego. Są to wymagania minimalne, więc może się zdarzyć, że służby IT Zamawiającego będą wymagały spełnienia dodatkowych warunków.

Z poważaniem

Signed by /
Podpisano przez:

Alicja Dudek

Date / Data:
2021-04-28
14:00

ENEA Centrum sp. z o.o.
Ul. Górecka 1
60-201 Poznań

NIP 777 00 02 843
REGON 630770227
www.enea.pl

Załącznik nr 1 - Wymagania bezpieczeństwa dot. kolokacji.
Otrzymują:
Adresat – email
EC

ENEA Centrum sp. z o.o.
Ul. Górecka 1
60-201 Poznań

NIP 777 00 02 843
REGON 630770227
www.enea.pl

Załącznik nr 1 - **Wymagania bezpieczeństwa dot. kolokacji**

Definicje pojęć użyte na potrzeby niniejszego dokumentu:

Centrum Przetwarzania Danych (CPD) – budowla lub zespół budowli przeznaczone do zgrupowania pomieszczeń, połączeń i obsługi techniki informacyjnej oraz sprzętu, sieci telekomunikacyjnych zapewniających usługi przechowywania, przetwarzania i dostarczania danych wraz z pełnym wyposażeniem i infrastrukturą do dystrybucji energii, zapewnienia parametrów środowiskowych oraz koniecznego poziomu odporności i zabezpieczeń wymaganych w celu zapewnienia pożądanej dostępności usług. **W niniejszym dokumencie CPD dot. usług kolokacji**.
Kolokacja – usługa udostępniania pomieszczeń i zasilania w usługi dodane związane z ciągłością działania.

Wymagania:

1. CPD powinny być budowane i wyposażone zgodnie z normami dla tego typu obiektów (m.in. ANSI/TIA-942 lub Uptime Institute), które definiują minimalne wymagania funkcjonalne i techniczne dla obiektów o różnej klasie bezpieczeństwa – **w przypadku ANSI/TIA-942 wymagany jest przynajmniej Tier-3, w przypadku Uptime Institute wymagany jest przynajmniej Tier-III**. Inne pomocne standardy, to rodzina norm PN-EN 50600.
2. Wspólnymi elementami wszystkich CPD muszą być :

   - konstrukcja budynku i nośność stropów zapewniająca możliwość umieszczenia w bezpieczny sposób sprzętu teleinformatycznego o typowych gabarytach i wadze;

   - drzwi wejściowe o wymiarach min. 1,0 m szerokości 2,13 m wysokości;

   - pomieszczenia kolokacyjne wyposażone w podłogę techniczną;

   - pomieszczenia kolokacyjne powinny posiadać systemy prowadzenia kabli zasilających i logicznych pod powierzchnią podnoszonej podłogi lub pod sufitem;

   - dedykowany niezawodnościowy system zasilania w energię elektryczną;

   - system zasilaczy awaryjnych UPS;

   - system klimatyzacyjny (rekomendowany zakres temperatur 18-27 C, wilgotność względna 30-60%);

   - system kontroli dostępu;

   - systemy przeciwpożarowe, w tym system gaszenia bezpieczny dla sprzętu elektronicznego (np. gazowy).
3. Wymaga się, aby obiekty CPD były ulokowane w miejscach nienarażonych na oddziaływania środowiskowe, zarówno naturalne (wykluczone są tereny zalewowe, zagrożone sejsmicznie itp.) oraz cywilizacyjne (obecność szkód górniczych, lotnisk, węzłów komunikacyjnych itp.), przy czym konkretne zalecenia w tym zakresie zależą od klasy Tier (w tym wypadku Tier-3 lub Tier-III) obiektu.
4. Budynek powinien być oddalony co najmniej o kilkadziesiąt metrów od ulicy czy większej drogi. Należy unikać sąsiedztwa dużych fabryk (zwłaszcza chemicznych), lotnisk, elektrowni. Lokalizacja powinna chronić przed powodzią, dlatego nie może znajdować się na terenie zalewowym, niekorzystne są również lokalizacje blisko cieków wodnych.
5. Wszelkie otwory technologiczne należy wykonać w takich miejscach, by nie było do nich bezpośredniego dostępu z zewnątrz.
6. Pomieszczenia CPD powinny być tak rozplanowane, by nie dopuścić do stworzenia miejsc, w których można łatwo ukryć przedmioty lub nawet osoby przed pracownikami ochrony i systemami nadzoru wizyjnego. Ponieważ takim miejscem jest podniesiona podłoga (w której znajdują się np. urządzenia związane z dystrybucją energii), należy zadbać o ochronę tej przestrzeni.
7. Zabezpieczenie terenu, wjazdów i wejść :

   - wokół budynku CPD powinien być utworzony pas buforowy. Teren powinien być ogrodzony i oświetlony. Aby utrudnić przełamanie zabezpieczeń przez samochody należy zastosować solidne ogrodzenie;

- każdy wjazd musi być wyposażony w bramy i zapory, które ochronią przed wtargnięciem na teren CPD. Przy wjazdach zaleca się stosowanie śluz, które uniemożliwią przejazd kilku samochodów jeden za drugim. Zasadniczym stanem bram i zapór powinno być ich zamknięcie, otwierane są przez obsługę dopiero po potwierdzeniu za pomocą systemu nadzoru i kontroli dostępu;

- aby ograniczyć miejsca nadzoru, budynek CPD powinien być wyposażony w jak najmniejszą liczbę wejść. Wejście na teren CPD może być dodatkowo zabezpieczone za pomocą urządzeń, takich jak kołowrotki, wyposażone w urządzenia identyfikujące. Ponieważ ochrona przeciwpożarowa wymaga wybudowania odpowiedniej liczby wyjść awaryjnych, należy zadbać o ich zabezpieczenie. Muszą być one łatwe do otwarcia od środka, trudne do sforsowania z zewnątrz, a każde ich otwarcie musi włączać alarm.

8. Dostęp do pomieszczeń nadzoru musi być chroniony tak samo jak wejście do CPD, a zarejestrowane obrazy powinny być rejestrowane poza obiektem CPD.

9. Dostęp do krytycznych obszarów, takich jak pomieszczenia CPD Zamawiającego, należy chronić za pomocą urządzeń dwuskładnikowego uwierzytelnienia. Można np. połączyć biometrię z kartami inteligentnymi.

10. Oprócz wynajmowanej powierzchni, Zamawiający powinien otrzymać (w zależności od zakresu usługi):

    - gniazda zasilające ~230V wraz z uzgodnionym przydziałem mocy i ewentualnie z podlicznikiem;

    - dedykowane okablowanie logiczne lub separację ruchu kierowanego do urządzeń Zamawiającego na poziomie przełącznika sieciowego;

    - sieć lokalną (private VLAN) lub dedykowane urządzenia LAN;

    - fizyczny dostęp do obiektu CPD;

    - możliwość skorzystania z pomieszczenia wyposażonego w dostęp konsolowy do serwerów umieszczonych w kolokacyjnym CPD;

    - umowy SLA na dostępność zasilania i usługi dodatkowe;

    - możliwość zestawienia dedykowanych łączy dzierżawionych od różnych operatorów;

11. Usługi dodatkowe oferowane jako uzupełnienie podstawowego zakresu usług kolokacji w CPD mogą obejmować (w zależności od podpisanej umowy) :

    - monitorowanie urządzeń Zamawiającego oraz sprawdzanie w trybie ciągłym dostępności usług;

    - powiadamianie przez e-mail, sms o ewentualnej awarii sprzętu;

    - comiesięczne raporty o ciągłości pracy urządzeń;

    - usługi typu „pomocna dłoń” (zdalne ręce);

    - usługi wsparcia inżynierów systemowych;

    - dostęp do Internetu;

    - mechanizmy ochrony i kontroli dostępu (ACL);

    - usługi bezpieczeństwa informacji (systemy firewall/ IDS, UTM, antywirusowe, antyspamowe, monitorowanie WWW);

    - usługi bezpieczeństwa dostępu, w tym przeciwdziałanie atakom DDoS;

    - utrzymanie i administracja siecią LAN na terenie CPD;

    - wydzielenie strefy dedykowanego dostępu;

    - monitoring dostępu poprzez karty zbliżeniowe;

    - monitoring wizyjny (CCTV) nadzorujący ciągi komunikacyjne wszelkie przejścia CPD, dostępy do poszczególnych szaf;

12. CPD dot. ciągłości działania powinny być umieszczone w budynkach oddalonych od siedziby Zamawiającego – w innej części miasta lub poza nim. Budynki takie powinny zapewniać anonimowość klienta oraz bezpieczeństwo fizyczne (np. ogrodzenie, ochrona).

13. Przebywanie w kolokacyjnym CPD – wymagane poziomy dostępów:

A – Eskortowany

Osoby na tym poziomie podlegają pełnej eskorcie przez cały okres pobytu na obszarze CPD. Nie mają prawa do samodzielnego poruszania się po obszarze CPD. Wejście na obszar CPD odbywa się po wyrażeniu zgody przez Zamawiającego. W trakcie pobytu na terenie CPD osoba z poziomem A ma obowiązek wylegitymować się dowodem osobistym bądź innym dokumentem potwierdzającym tożsamość na każde żądanie uprawnionego pracownika CPD.

B – Nieeskortowany

Pracownikom Zamawiającego, którzy w zakresie obowiązków mają obsługę infrastruktury Zamawiającego zlokalizowanej w kolokowanym CPD, nadaje się nieograniczony czasowo pełen dostęp do przestrzeni CPD zajmowanych przez Zamawiającego. Osoby te zobowiązane są do wylegitymowania się na żądanie uprawnionego pracownika CPD.

C – Dostawcy/Serwis/Support

W przypadku realizowania inwestycji/serwisu/supportu bądź dostaw sprzętu na obszarze kolokowanego CPD dopuszcza się nadanie Dostawcy/Serwisowi/Supportowi dostępu na poziomie B z zastrzeżeniem, iż musi to wynikać z wcześniejszych ustaleń. W pozostałym przypadku zostanie nadany dostęp na poziomie A.

D – Goście

Goście są dopuszczani po zatwierdzeniu przez Zamawiającego, z zastrzeżeniem, iż informacja o planowanej wizycie gościa musi być przekazana przez organizatora z kilkudniowym wyprzedzeniem. Goście mają status A wraz ze wszystkimi zastrzeżeniami.

E – Pozostali pracownicy Zamawiającego

Pracownicy Zamawiającego, którzy w swoim zakresie obowiązków nie mają pracy w obszarze kolokowanego CPD, a z powodów realizacji zadań służbowych muszą wejść na obszar kolokowanego CPD podlegają dostępowi na poziomie A. Dodatkowo, nadzór CPD jest zobowiązany odnotować jaki zakres prac był wykonywany.

Osoby z dostępem A, C, D, E są osobami nieupoważnionymi do samodzielnego przebywania na terenie kolokowanego CPD.

14. Zasady prowadzenia prac na terenie kolokowanego CPD

    Wszelkie prace oraz czynności mające potencjalny wpływ na działanie infrastruktury CPD w części kolokacyjnej należy uprzedzić stosownym wnioskiem/prośbą u Zamawiającego. Do takich prac należy zaliczyć:

    - montaże lub demontaże nowych elementów infrastruktury i okablowania strukturalnego;

    - dołączanie lub odłączanie urządzeń bezpośrednio do infrastruktury elektrycznej;

    - wszelkie prace wykonywane przez firmy zewnętrzne;

    - w zależności od daty planowanego montażu, urządzenia należy składować w magazynie lub pomieszczeniu technicznym. Pokój techniczny powinien być przestrzenią technologiczną służącą do rozpakowania i przygotowania sprzętu teleinformatycznego do instalacji.

15. System okablowania strukturalnego CPD powinien zostać zbudowany w oparciu o wytyczne zawarte w normach:

    - TIA – 942 Infrastruktura telekomunikacyjna dla Data Center

    - ISO 20000

    - BS 15000

    - TIA/EIA 606

16. System zasilania w CPD powinien być zbudowany tak, by istniała możliwość zasilania infrastruktury IT z dwóch zewnętrznych, niezależnych, przełączanych automatycznie linii energetycznych.

17. Dla prawidłowej budowy sieci zasilania elektrycznego powinno się stosować jeden ze standardów zasilania TIER.

18. Dla podniesienia bezpieczeństwa CPD należy stosować niezależne przyłącza energetyczne np. dwa niezależne transformatory zasilane z odrębnych sieci dystrybucyjnych.

19. Przy wyborze generatora prądu należy pamiętać o:

    - mocy agregatu przy uwzględnieniu prądów rozruchowych zasilanych urządzeń;

    - pojemności zbiornika oraz wartości spalania, od których zależy bezobsługowy czas autonomii instalacji zasilającej;

    - optymalnej lokalizacji urządzenia, zagadnienie to jest niezmiernie ważne m.in. ze względu na poziom emitowanego hałasu i zanieczyszczeń, konieczność dostarczania tlenu atmosferycznego oraz ochrony urządzenia przed czynnikami atmosferycznymi i uszkodzeniem. Może być zrealizowane np. przez zastosowanie wyciszonego kontenera zewnętrznego.

    - pożądana funkcjonalność to możliwość tankowania urządzenia „w locie", podczas pracy urządzenia jak również możliwość zdalnego monitorowania i zarządzania pracą urządzenia np. poprzez protokół SNMPv3.

20. Rozdzielnia główna niskiego napięcia (punkt styku instalacji obiektowej ze źródłem/źródłami zasilania) powinna być wyposażona w bezpieczne układy przełączające SZR, analizatory sieci, a także bezpieczniki główne.

21. Należy stosować UPSy typu „online".

22. Zaleca się by UPS wyposażony był w by-pass pozwalający na wypięcie urządzenia z instalacji na czas naprawy/przeglądu. Pożądaną funkcjonalnością jest możliwość zdalnego monitorowania i zarządzania pracą urządzenia np. poprzez protokół SNMPv3.

23. Czas podtrzymania UPSa powinien gwarantować czas rozruchu generatora prądowego (czas po którym generator dostarcza stabilne napięcie o docelowej mocy) lub przełączenia pomiędzy podstawowymi źródłami zasilania.

24. UPSy powinny być urządzeniami o podwójnej konwersji zasilania, co oznacza, że ewentualne zakłócenia w sieci energetycznej nie wpłyną na jakość zasilania serwerów.

25. Większość urządzeń stosowanych w CPD powinna być wyposażona w min. dwa moduły zasilające i pożądane jest, aby były one podłączone do niezależnych obwodów w ramach instalacji.

26. Systemy bezpieczeństwa fizycznego w CPD, które należy uwzględnić :

    - systemy kontroli dostępu;

    - systemy sygnalizacji włamania i napadu;

    - systemy p. poż. i gaszenia pożarów;

    - systemy telewizji przemysłowej oraz dozorowej.

27. Szyby okienne w pomieszczeniach CPD powinny posiadać klasę odporności na przestrzelenie co najmniej S3 według norm EN 356 i DIN 52 290.

28. Drzwi wejściowe do CPD powinny spełniać wymagania klasy „B" według PN-90/B92270, a zamki kluczowe – wymagania klasy „B" lub „C" wg PN-88/B-94399.

29. Czas reakcji służby ochrony na sygnały alarmu nie powinien być dłuższy niż 8 min.

30. Wszystkie osoby podejmujące próbę dostępu do zasobów informacyjnych CPD powinny być zidentyfikowane i opcjonalnie powinna nastąpić ich autoryzacja w systemie informatycznym.

31. System ochrony fizycznej powinien nadzorować i rejestrować, z wykorzystaniem kamer, ruch przed wejściem do pomieszczenia chronionego umożliwiając przeglądy (kontrole) tych działań.

32. Systemy kontroli dostępu i sygnalizacji włamania oraz telewizji dozorowej powinny umożliwiać m.in.:

    - wizualizację;

    - nadawanie uprawnień;

    - backup bazy danych;

    - podgląd monitoringu wizyjnego.

33. W ramach ochrony przeciwpożarowej w CPD powinny być wykorzystywane trzy poziomy zabezpieczeń:

    - system sygnalizacji pożaru;

    - system gaszenia gazem – np. FM 200, urządzenie gaśnicze TA200;

    - system wczesnej detekcji dymu VESDA.

34. W pomieszczeniach CPD nie może być jakichkolwiek instalacji:

    - wodno-kanalizacyjnych;

    - centralnego ogrzewania;

    - gazowych.

    Mogłyby one stwarzać zagrożenie dla systemów serwerowych.

35. Aby zachować oczekiwaną funkcjonalność systemów oraz co ważniejsze zapewnić zakładany poziom bezpieczeństwa obiektu/usług należy regularnie serwisować/konserwować infrastrukturę fizyczną CPD. Szczególnej kontroli powinny podlegać systemy/elementy krytyczne z punktu widzenia bezpieczeństwa czy dostępności obiektu. Dla przykładu są to baterie zasilaczy UPS, obciążone elementy rozdzielni elektrycznych, szczelność układu klimatyzacji oraz szczelność systemu gaszenia.

36. Wymaga się minimum następujących funkcji bezpieczeństwa dla przełączników pracujących w warstwie 3 sieci :

    - uwierzytelnianie urządzeń z wykorzystaniem protokołu 802.1x;

    - wymuszanie polityk bezpieczeństwa (funkcje wykorzystywane przez systemy Network Access Control);

    - zabezpieczenie przed przyłączaniem nieautoryzowanych serwerów lub podszywaniem się pod inne urządzenia sieci (ataki MAC lub IP Spoofing).

37. Główne zabezpieczenia jakie powinny posiadać serwery w CPD :

    - redundantne zasilanie;

    - redundantne interfejsy sieciowe;

    - redundantne pamięci masowe;

    - możliwość wymiany kluczowych modułów bez konieczności ich wyłączania (technologie hot plug i hot swap).

38. Koniecznym elementem CPD jest podłoga techniczna.

39. Pozostałe zabezpieczenia elektryczne budynku CPD :

    Budynek musi być zasilany z dwóch niezależnych linii energetycznych, musi posiadać zabezpieczenia przeciw-przepięciowe, przeciw-porażeniowe, odgromowe (w kategorii C).

40. Każdorazowa próba dostania się do pomieszczenia kolokowanego CPD musi być odnotowywana w systemie kontroli dostępu.

41. Budynek/budynki, w którym/ch znajduje się CPD muszą być chronione 24h na dobę 7 dni w tygodniu przez co najmniej jednego pracownika ochrony budynku. Przez cały czas w budynku/budynkach CPD musi znajdować się minimum jeden pracownik ochrony.

42. Wszelkie pomieszczenia CPD zawierające sprzęt telekomunikacyjny, serwery oraz pomieszczenie UPS'ów muszą być klimatyzowane w systemie N+1 (nadmiarowa klimatyzacja), dzięki czemu awaria urządzenia klimatyzacyjnego nie narazi sprzętu na przegrzanie.

43. Napięcie zasilania serwerów powinno podlegać monitoringowi. W przypadku jego zaniku lub niestandardowych parametrów pracy administratorzy dyżurni powinni być o tym powiadamiani.

44. Serwery w CPD powinny znajdować się w specjalnie wyizolowanej sieci w celu ograniczenia dostępu do nich osób nieupoważnionych. Dostęp do tej sieci powinien być ograniczony zarówno z sieci Internet jak i ze wszystkich sieci wewnętrznych. Dostęp powinien wymagać specjalnych uprawnień (np. na firewallach Zamawiającego).

45. CPD powinno posiadać nadmiarowość łącz danych (minimum dwóch łącz telekomunikacyjnych od dwóch niezależnych dostawców).

46. Wejście, wyjście i wnoszenie sprzętu – zasady :

    - przed wejściem do CPD i po jego opuszczeniu należy zgłosić się do ochrony celem weryfikacji uprawnień do wejścia i ewidencji pobytu. Weryfikacja odbywa się na podstawie dowodu tożsamości (np. dowodu osobistego);

    - wnoszenie sprzętu komputerowego i telekomunikacyjnego, który będzie zainstalowany w CPD, jest ewidencjonowane. Należy poinformować o tym administratora lub ochronę obiektu podczas ewidencji wejścia;

    - wynoszenie sprzętu komputerowego i telekomunikacyjnego zdemontowanego z CPD jest ewidencjonowane, należy o tym poinformować administratora lub ochronę obiektu przy wyjściu;

    - osoba, która ma dostęp do CPD Zamawiającego, powinna być przynajmniej trzy razy sprawdzona przed uzyskaniem dostępu. Kontrola może zostać przeprowadzona przy drzwiach zewnętrznych, wewnętrznych (separujących gości od pracowników i serwisantów) oraz przy wejściu do krytycznych obszarów. Do kontroli w tym ostatnim miejscu należy zastosować konstrukcje zapobiegające wejściu osoby bez jej pozytywnego uwierzytelnienia (na przykład kołowrotki lub śluzy). Wejście w tę strefę powinno wymagać wcześniejszego zgłoszenia potrzeby dostępu.

47. Zakazuje się :

    - wstępu do stref, do których nie udzielono pozwolenia;

    - spożywania, wnoszenia posiłków oraz napojów do CPD;

    - rejestracji obrazu i dźwięku bez zezwolenia;

    - opierania się o jakiekolwiek elementy infrastruktury serwerowni np.: przyciski ppoż, obudowy szaf serwerów i innych urządzeń, włączników, przełączników w obszarze CPD;

    - manipulowania przy urządzeniach, bądź instalacjach, do których nie posiada się zgody, uprawnień.