Planowanie zachowania ciągłości

- **Zarządzanie ciągłością działania –** całościowy proces zarządzania, który identyfikuje zagrożenia dla organizacji oraz wpływ tych zagrożeń. Określa strukturę dla budowania organizacyjnej odporności uwzględniając zabezpieczenia dla najważniejszych procesów zachodzących w organizacji.

- **Ciągłość działania** – przeciwdziałanie przerwom w działalności biznesowej oraz ochrona krytycznych procesów biznesowych przed rozległymi awariami systemów informacyjnych lub katastrofami oraz zapewnienie wznowienia działalności w wymaganym czasie.

- **Plan zachowania ciągłości** – udokumentowana procedura określająca reakcję na zakłócenie ciągłości i sposób przywrócenia zdolności działania na wcześniejszych parametrach.

- **Business Continuity** – zapewnianie ciągłości działania organizacji

- **Information Technology Contingency** – zapewnianie ciągłości działania systemom informatycznym

Planowanie zachowania ciągłości

- **Disaster Recovery** – odtwarzanie systemów informatycznych po katastrofie
- **Analiza wpływu** – proces analizy działań i ich skutków mających wpływ na biznes z powodu przerwy w działaniu
- **Incydent** – sytuacja będąca lub mogąca prowadzić do przerwy, straty, awarii lub kryzysu
- **Infrastruktura** – system urządzeń, sprzętu i usług niezbędnych do działania organizacji
- **MAO (maximum acceptable outage)/MTPD (maximum tolerable period of disruption)/MTD** – maksymalny czas niedostępności usługi lub zasobu, zanim organizacja poniesie nieakceptowalne konsekwencje
- **MBCO/MALS (maximum tolerable period of disruption/Minimum Acceptable Levels of Service)** – minimalny poziom lub ilość oczekiwanych usług niezbędnych dla organizacji podczas zakłócenia lub przerwy działania

Planowanie zachowania ciągłości

- **RTO (recovery time objective)** – okres czasu w wyniku incydentu, w którym usługa, produkt, działalność lub zasoby powinny być przywrócone
- **RPO (recovery point objective)** – punkt do którego powinna być przywrócona informacja/dane, aby funkcjonować po wznowieniu działania
- **RTA (recovery time actual)** – ustalany poprzez testy czas przywrócenia stanu systemu sprzed wystąpienia awarii
- **NRO (network recovery objective)** – okres czasu niezbędny dla odzyskania sprawności połączeń sieciowych
- **BWO (backup window objective)** – długość przerwy w dostarczaniu usług/informacji niezbędna w celu wykonania kopii zapasowej
- **MDL (maximum data loss)** – maksymalna wielkość danych utraconych w wyniku incydentu uwzględniająca możliwości odtworzenia ze źródeł spoza systemu
- **Zasoby**–aktywa, ludzie, informacje, technologia niezbędne do osiągania celów przez organizację

Planowanie zachowania ciągłości

Norma ISO 17799 zawiera ponad 130 zasad dot. bezpieczeństwa informacji zgrupowanych w 12 obszarów:

- Szacowanie ryzyka
- Polityka bezpieczeństwa
- Organizacja bezpieczeństwa
- Zarządzanie aktywami
- Bezpieczeństwo zasobów ludzkich
- Bezpieczeństwo fizyczne i środowiskowe
- Zarządzanie systemami i sieciami
- Kontrola dostępu do systemu
- Rozwój i utrzymanie systemu
- Zarządzanie incydentami
- Zarządzanie ciągłością działania
- Zgodność z regulacjami prawnymi

Planowanie zachowania ciągłości

➢Zarządzenie ciągłością działania (punkt 14 PN-ISO/IEC 17799:2007)

Zaleca się uwzględnienie w szczególności elementów:

- Sformułowanie i udokumentowanie planów zapewnienia ciągłości działania określających wymagania bezpieczeństwa informacji zgodnie z uzgodnioną strategią ciągłości działania
- Regularne testowanie i aktualizowanie przyjętych planów i procesów
- Zaleca się określenie zdarzeń (lub ciągów zdarzeń), które mogą spowodować przerwy procesów biznesowych organizacji np.: awarie sprzętu, błędy ludzkie, kradzież, pożar, katastrofy naturalne oraz akty terroryzmu.
- Zaleca się przeprowadzenie szacowania ryzyka, aby określić prawdopodobieństwo wystąpienia takich przerw oraz ich wpływ, uwzględniając: ramy czasowe, rozmiar szkód oraz czas odtwarzania

Planowanie zachowania ciągłości

➢ **Plan zachowania ciągłości – struktura**

- **Warunki** uruchomienia planu (np. Jak oceniać sytuację, kto ma być zaangażowany)
- **Procedury awaryjne**, opisujące działania podejmowane po incydencie
- **Procedury odtwarzania** opisujące działania podejmowane przy przywracaniu procesów systemów w wymaganym czasie
- **Procedury** utworzenia tymczasowego obejścia
- **Procedury wznowienia** opisujące przywrócenie normalnych operacji w systemie
- Harmonogram testów planu
- Zakresy odpowiedzialności osób
- **Krytyczne aktywa i zasoby** potrzebne do wykonania procedur awaryjnych, odtwarzania i wznowienia

Planowanie zachowania ciągłości

➢Plan zachowania ciągłości – testowanie

- Testowanie scenariuszy na „papierze”
- Symulacje
- Testowanie w zakresie systemów technicznych
- Testowanie odtworzenia w lokalizacji zapasowej
- Próby generalne

POLITECHNIKA RZESZOWSKA
im. IGNACEGO ŁUKASIEWICZA

Procedury bezpieczeństwa

Opis procesu	Nazwa dokumentu
Struktura zarządzania	Zarządzanie dokumentacją
Zarządzanie ryzykiem	Karta ryzyka
Zarządzanie ryzykiem	Metodologia szacowania ryzyka
Zarządzanie ryzykiem	Procedura szacowania ryzyka
Zarządzanie ciągłością	Disaster Recovery Plan
Zarządzanie ciągłością	Business Impact Analysis
Zarządzanie ciągłością	Plany zachowania ciągłości działania
Zarządzanie ciągłością	Instrukcje tworzenia kopii bezpieczeństwa
Zarządzanie ciągłością	Schemat kopii zapasowych
Zarządzanie dostępnością i pojemnością	Procedura zarządzania pojemnością systemu
Zarządzanie zmianami	Procedura nadzoru nad zmianami i konfiguracją
Zarządzanie operacjami	Procedury eksploatacyjne i utrzymaniowe systemu

POLITECHNIKA RZESZOWSKA
im. IGNACEGO ŁUKASIEWICZA

Procedury bezpieczeństwa

Opis procesu	Nazwa dokumentu
Zarządzanie bezpieczeństwem	Polityka bezpieczeństwa systemu
Zarządzanie bezpieczeństwem	Procedura niszczenia nośników danych
Zarządzanie bezpieczeństwem	Regulaminy użytkowników
Zarządzanie bezpieczeństwem	Procedura obsługi incydentów bezpieczeństwa
Zarządzanie bezpieczeństwem	Schemat sieci
Zarządzanie bezpieczeństwem	Procedura zarządzania kontami i uprawnieniami
Zarządzanie bezpieczeństwem	Standard bezpieczeństwa przełączników sieciowych
Zarządzanie bezpieczeństwem	Standard bezpieczeństwa serwerów (pod kątem funkcji)
Zarządzanie bezpieczeństwem	Standard bezpieczeństwa routerów i firewalli
Zarządzanie bezpieczeństwem	Standard bezpieczeństwa aplikacji (funkcja, architektura)
Monitorowanie	Procedura monitorowania systemu

Procedury bezpieczeństwa

➢Procedura kontroli dostępu do systemu

- Architektura systemu: system operacyjny, aplikacja i baza danych (nazwy i wersje)
- Połączenia w sieci LAN/WAN: dostępność z sieci wewnętrznej i zewnętrznej
- Wymiana danych pomiędzy systemami
- Uwzględniamy zabezpieczenia:
  - Sieci
  - Systemu
  - Aplikacji
  - Organizacyjne
- Zabezpieczenia na poziomie sieci:
  - ACL
  - Filtrowanie pakietów
  - Zasady routingu
  - Podział na podsieci
  - Segmenty VLAN

Procedury bezpieczeństwa

➢ Procedura kontroli dostępu do systemu

- Zabezpieczenia na poziomie systemu i aplikacji:
  - Sposób uwierzytelniania użytkowników
  - Grupy uprawnień w aplikacji i systemie
  - Kontrolki dostępu do poszczególnych elementów sytemu
  - Dostęp do baz danych
- Organizacyjne:
  - Sposób zapewnienia, że do informacji mają dostęp wyłącznie upoważnione osoby
  - Opis zabezpieczeń -identyfikacji użytkownika (konta użytkowników, hasła, karty)
  - Sposób wnioskowania, nadawania, zmiany i odbierania uprawnień
  - Instrukcja tworzenia kont użytkowników w systemie
  - Kontrola dostępu do pomieszczeń ze zasobami systemu (serwery, telekomunikacja)
  - Dokumentacja ról w systemie
  - Czasowa aktywacja uprawnień, opis czasu ważności kont
  - Zasady haseł, rotacja haseł, zasady tworzenia haseł, minimalna długość

➢ Procedura kontroli dostępu do systemu

- Formularze:
  - Wniosek o założenie/zmianę/usuniecie
  - Wykaz praw dostępu – role dostępu
  - Sposób przesyłania haseł do użytkownika
  - Rejestr użytkowników systemu

➢ Procedura kontroli dostępu do systemu

Rola	System	Rodzaj informacji	Uprawnienia
Adam Król	Nazwa danego systemu	Wszystkie wynikające z zakresu obowiązków lub zadania	Odczyt
		Własne konto i hasło	Odczyt, Zamiana
Jan Nowak	Nazwa danego systemu	Wszystkie wynikające z zakresu obowiązków lub zadania	Odczyt, Zamiana
		Własne konto i hasło	Odczyt, Zamiana
Piotr Obrzut	Nazwa danego systemu	Wszystkie wynikające z zakresu obowiązków lub zadania	Odczyt, Zamiana, Tworzenie, Kasowanie
		Własne konto i hasło	Odczyt, Zamiana

➢ Procedura obsługi incydentów bezpieczeństwa

• Identyfikacja incydentów:

- Duże obciążenie łącza internetowego
- Utrata dostępu do usługi, urządzenia lub części lub całości funkcjonalności
- Nieautoryzowana modyfikacja, zniszczenie, zmiana, utrata danych
- Anomalie w systemie
- Wykorzystanie oprogramowania z nieznanych, niesprawdzonych źródeł
- Blokada logowania
- Niestabilna praca systemu
- Nadmierne w stosunku do wykonywanych zadań (zakres upoważnień) uprawnienia użytkownika do zasobów systemu
- Praca w systemie poza zwykłymi godzinami dla określonych osób
- Nieznane konta użytkowników
- Wyższa od średniej aktywność procesów, kont lub usług sieciowych
- W określonym czasie duża liczba nieudanych prób logowania

Procedury bezpieczeństwa

➢ Procedura obsługi incydentów bezpieczeństwa

• Rodzaje incydentów:

- Nieupoważniony dostęp oraz modyfikacja, zmiana, zniszczenie lub usunięcie danych
- Udostępnianie danych osobom nieupoważnionym
- Omijanie zabezpieczeń
- Niedopełnienie obowiązku ochrony danych
- Otwarcie nieautoryzowanego kanału komunikacyjnego umożliwiającego interakcję z danymi
- Przetwarzanie danych ze źródła nielegalnego
- Nie podjęcie działań zmierzających do eliminacji zidentyfikowanego zagrożenia
- Ujawnienie lub umożliwienie dostępu do haseł osobie nieupoważnionej
- Przesyłanie poza sieć wewnętrzną informacji chronionych bez zabezpieczenia
- Kradzież nośników z danymi
- Kradzież sprzętu informatycznego
- Spowodowanie utraty danych np. Poprzez nie wykonanie kopii zapasowych
- Niszczenie nośników niezgodnie z regulacjami wewnętrznymi

➢ Procedura obsługi incydentów bezpieczeństwa

• Reakcja na incydent:

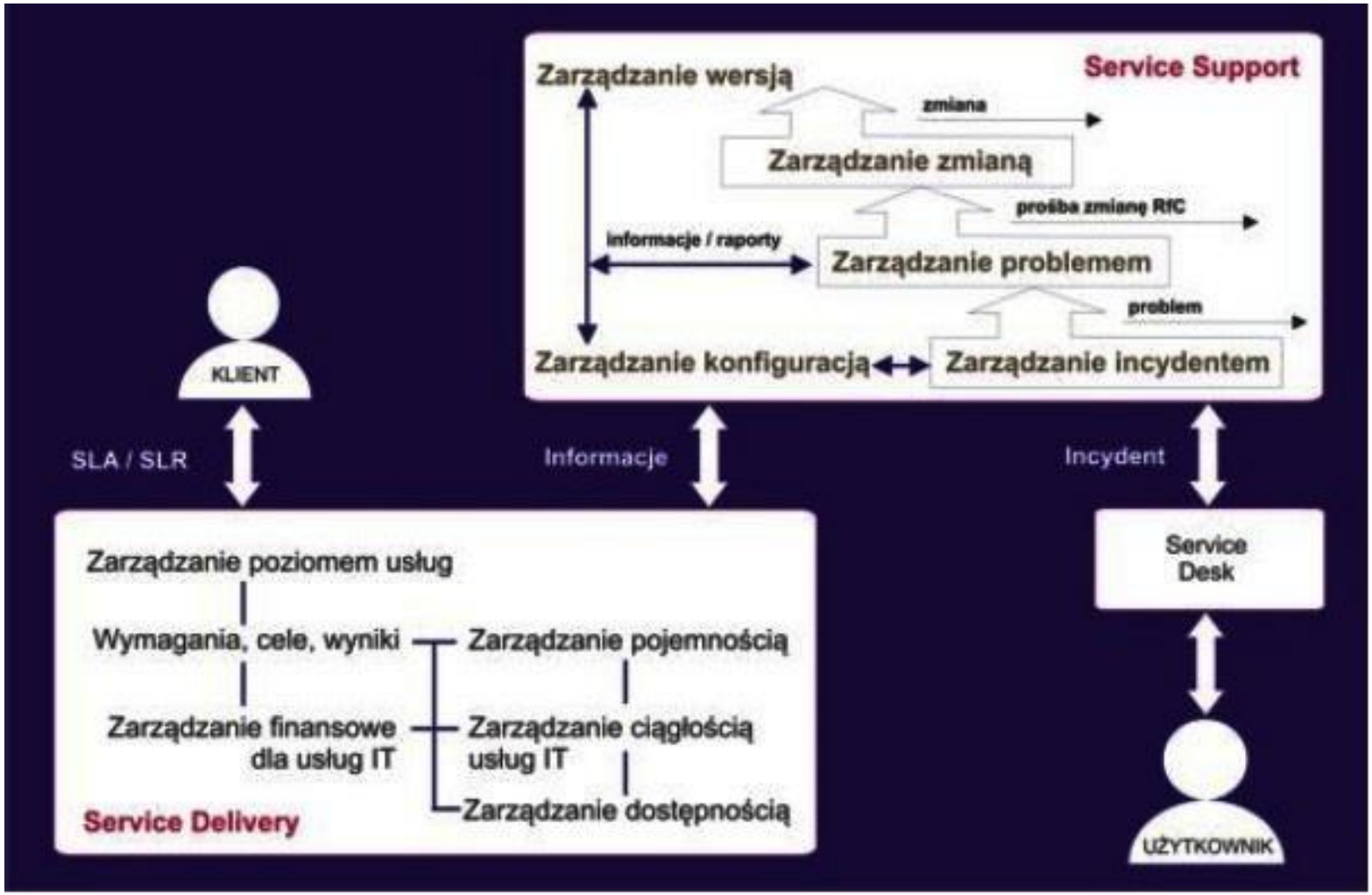
- Administrator ma obowiązek zareagować na alarm:
  - Wykryty w logach
  - Wygenerowany przez IPS
  - Przesłany przez systemy automatycznie powiadamiające o zdarzeniach
  - Przekazany przez użytkownika
- Oszacowanie czasu poszczególnych działań po incydencie
- Zabezpieczenie materiału dowodowego
- Poszukiwanie dowodów na nośnikach elektronicznych
- Poszukiwanie i zbieranie dowodów
- DD – tworzenie obrazów dysków
- DCFLDD – tworzenie obrazów dysków
- Md5sum – określanie skrótu, sumy kontrolnej
- Fastsum – określanie skrótu, sumy kontrolnej
- Firemost – odzyskiwanie skasowanych plików

Procedury bezpieczeństwa

➢ Procedura obsługi incydentów bezpieczeństwa

- Sposób zgłaszania zdarzeń związanych z bezpieczeństwem systemu
- Zasady odpowiedzi na incydent
- Zasady eskalacji incydentu
- Działania po zgłoszeniu incydentu
- Ogłoszenie miejsca zgłaszania incydentów
- Proces zwrotnego informowania zgłaszających
- Wskazanie narzędzi do zgłoszeń incydentów:
  - Telefon
  - Formularz
  - Aplikacja
  - E-mail
- Zanotowanie wszystkich ważnych szczegółów zdarzenia: rodzaju incydentu, błędu działania systemu, wiadomości z ekranu, osobliwego zachowania
- Zakaz dla użytkowników podejmowania jakichkolwiek własnych działań, obowiązek natychmiastowego zgłoszenia właściwym osobom
- Zabezpieczenie dowodów po incydencie
- Określenie postępowania dyscyplinarnego

Procedury użytkownika



Procedury użytkownika

Service Desk – zakres funkcji:

- Zachowanie ciągłości działania
- Wsparcie użytkowników zgodnie z określonymi czasami reakcji i rozwiązania
- Odbiór, ewidencja i nadawanie priorytetów incydentom i zapytaniom
- Obsługa lub przekazywanie zgłoszeń
- Dokumentacja wszystkich zgłoszeń i zapytań
- Przywracanie działania usług
- Śledzenie incydentów i rozwiązań
- Zapobieganie naruszeniom parametrów poziomu SLA
- Informowanie użytkowników o statusie zgłoszeń
- Przejmowanie zadań z innych procesów np. konfiguracji czy zarządzania incydentami
- Raportowanie jakości usług IT, satysfakcji użytkowników i kosztów

Procedury użytkownika

➢ Obsługa Service Desk – zakres procedury:

- Call Center – ewidencja i przekazanie.
- Help Desk – ewidencja, rozwiązanie i/lub przekazanie.
- Service Desk – to samo co Help Desk, ale w zakresie są wszystkie zgłoszenia
- Priorytet – określenie priorytetu obsługi incydentu
- Eskalacja incydentu
  - W strukturze funkcjonalnej (zasoby)
  - W hierarchii
- Service Request – zapytanie o usługę (nie incydent, nie awaria krytyczna)
- Incident – zdarzenie nie będące standardowym działaniem usługi
- Estymacja priorytetów zależy od:
  - Wpływu na minimalny poziom danej usługi
  - Wpływu na ciągłość działania procesu biznesowego
  - Pilności rozumianej jako wymaganą szybkość rozwiązywania problemu (incydentu)
- Priorytet jest sumą wpływu i pilności

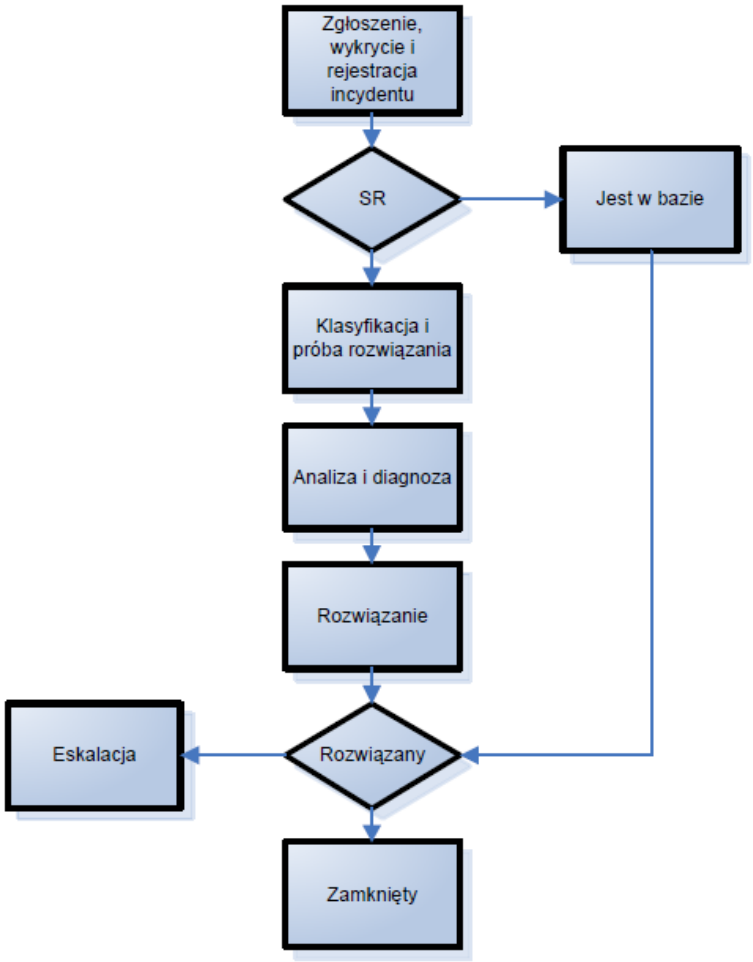
Procedury użytkownika

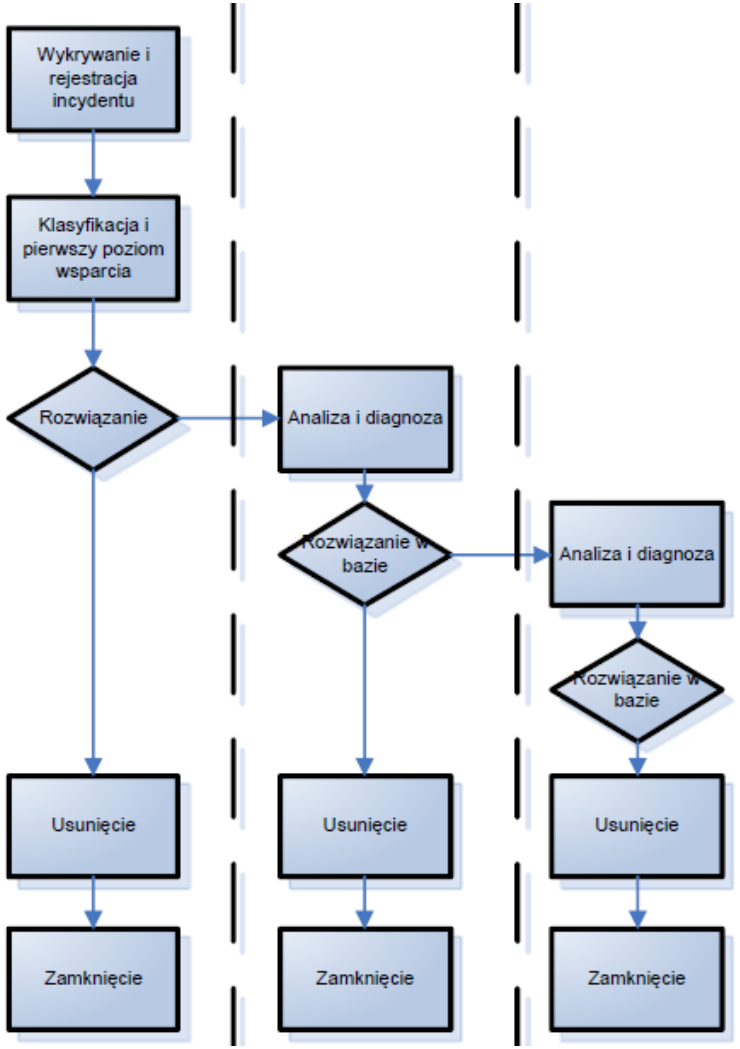
- **Obsługa Service Desk – zakres procedury:**

  • Eskalacja incydentu:
    • Do wyższego poziomu personelu
    • Kierownik SD, CIO, Zarząd
    • Wymaganie zastosowania dodatkowych zasobów w celu rozwiązania problemu
    • Drugi poziom wsparcia – specjaliści o większej wiedzy niż pracujący na pierwszym poziomie
    • Trzeci poziom wsparcia – specjaliści firm zewnętrznych np.support producenta bazy danych lub aplikacji

Procedury użytkownika

- **Obsługa Service Desk – zakres procedury:**





Procedury użytkownika

➢ Obsługa Service Desk – zakres procedury:

- Obsługa incydentu:
  - Rejestracja: ID, data, czas
  - Klasyfikacja
  - Ocena wpływu (przerwa, strata finansowa) i pilności (godziny pracy, koniec miesiąca)
  - Uwzględnienie priorytetu użytkownika
  - Sprawdzenie rozwiązań w bazie wiedzy
  - Sprawdzenie istnienia obejścia, rozwiązania tymczasowego
  - Eskalacja do 2 i 3 poziomu wsparcia
  - Bieżąca aktualizacja stanu zgłoszenia/incydentu
  - Rejestracja rozwiązania
  - Zamknięcie incydentu po potwierdzeniu prawidłowego działania usługi

Procedury użytkownika

Regulamin użytkownika:

- Definicje podstawowych pojęć
- Zakres stosowania
- Wykaz informacji chronionych i ich właścicieli
- Wykaz systemów i ich właścicieli
- Zasady korzystania z informacji chronionych
- Zasady ochrony danych w systemach teleinformatycznych
- Zasady korzystania z zasobów Internetu
- Zasady użytkowania nośników
- Zasady korzystania z komputerów przenośnych
- Zasady dostępu i ochrony pomieszczeń z urządzeniami systemu teleinformatycznego
- Zasady udostępniania danych z systemu
- Monitorowanie systemu i użytkownika
- Odpowiedzialność za naruszenia
- Oświadczenie pracownika o zachowaniu poufności
- Oświadczenie osoby zewnętrznej o zachowaniu poufności

Procedury użytkownika

- **Struktura standardu:**

  - Realizacja wymagań – kolejność oraz wskazanie wymagań w zakresie zgodności
  - Wymagania konfiguracyjne:
    - Zasady dotyczące minimalnego poziomu usług
    - Określenie protokołów sieciowych
    - Zdefiniowanie wymogów dla list ACL
    - Definicja segmentów sieci
    - Wymagania dla kopii zapasowych
    - Zasady routingu w sieciach
    - Wymagania kompatybilności z innymi urządzeniami i systemami
    - Łączenie z innymi urządzeniami

Procedury użytkownika

Struktura standardu:

- Wymagania instalacyjne:
  - Zgodność z certyfikatami
  - Poziom SLA
  - Zapewnienie kompatybilności z pozostałymi urządzeniami w sieci
  - Upgrade firmware przed pierwszym użyciem urządzenia
  - Zmiana haseł domyślnych na zgodne z polityką haseł
  - Usunąć lub wyłączyć konta domyślne
  - Utworzyć osobne konta dla pracowników firm zewnętrznych w celu konfiguracji lub obsługi outsourcingowej.
  - Utworzenia dokumentacji w zakresie połączeń oraz struktury podsieci i VLAN. Wprowadzić standard oznaczeń krosowanych gniazd sieciowych.
  - Utworzenie procedur administracyjnych z obowiązkiem stałej aktualizacji.
  - Zasady przechowywania w miejscach bezpiecznych np. metalowa szafka, sejf :
    - kopii zapasowych konfiguracji
    - dokumentacji technicznej
    - procedur

Procedury użytkownika

Struktura standardu:

- Zasady administracji:
  - W celu zarządzania urządzeniami należy korzystać tylko z VLAN wydzielonego od pozostałych segmentów sieci.
  - Podczas zarządzania i konfiguracji zdalnej należy korzystać w protokołów szyfrowanych.
  - Dostęp do portów konfiguracyjnych powinien być filtrowany adresów źródłowych.
  - Należy stosować ograniczenie czasu podtrzymywania sesji bezczynnej np. 20 minut.
  - Podłączanie komputerów powinno wymagać uwierzytelnienia realizowanego na wejściu portu przełącznika.
  - Polityki dostępowe powinny być przeglądane minimum 1 raz w roku.
  - Logi urządzenia powinny być przekierowane do kolektora zdarzeń znajdującego się w innym segmencie sieci.

Procedury użytkownika

- **Struktura standardu:**

• Zasady administracji:
  • Segmenty VLAN powinny być tworzone ze względu na podział funkcjonalny.
  • Dokumentacja urządzenia powinna być prowadzona przez administratora w zakresie zawierającym w szczególności:
    – Mapa VLANów.
    – Reguły ACL.
    – Konfiguracja portów fizycznych.
    – Spis otwartych portów.
    – Tablica routingu.
    – Pełną konfiguracją w postaci pliku na nośniku zewnętrznym tworzoną np. poprzez polecenie show running-config.

Procedury użytkownika

Struktura standardu:

- Zapewnienie ciągłości działania:
  - Należy zachowywać ciągłość działania zgodnie z Procedurą Zarządzania Ciągłością Działania.
  - Dla przełączników należy stosować redundancję zasilaczy oraz UPS.
  - Należy stosować redundancję urządzeń w postaci połączeń stackowych. Należy również posiadać jedno nadmiarowe urządzenie danego typu i modelu, które jest uruchamiane w razie awarii produkcyjnego urządzenia.
  - Urządzenia powinny być eksploatowane w parametrach środowiska zgodnych z zaleceniami producenta (np. temperatura, wilgotność).
  - Konserwacja urządzeń sieciowych powinna być realizowana nie rzadziej niż raz do roku.

Procedury użytkownika

Struktura standardu:

- Wymagania bezpieczeństwa fizycznego:
  - W pomieszczeniach z przełącznikami powinny być stosowane drzwi o podwyższonej odporności na włamanie oraz ogień.
  - Fizyczny dostęp do pomieszczeń powinien być kontrolowany przez system kontroli dostępu.
  - Należy stosować monitoring wejścia do pomieszczeń z minimum dwóch niezależnie podłączonych kamer przemysłowych.
  - Do pomieszczenia może mieć dostęp wyłącznie upoważniony personel.
  - Należy zapewnić, że personel jest przeszkolony z używania stosowanego sprzętu gaśniczy.
  - W pomieszczeniu należy monitorować parametry środowiska – temperaturę oraz wilgotność.

Procedury użytkownika

- **Struktura standardu:**

• Wymagania audytu – etapy audytu:.

– Weryfikacja bezpieczeństwa fizycznego.

– Weryfikacja bezpieczeństwa portów konfiguracyjnych.

– Sprawdzenie wydajności.

– Weryfikacja zgodności instalacji z niniejszym standardem.

• Wymagania audytu – wymagania testów technicznych:

– Ataki na protokoły DHCP i ARP.

– Ataki na VLAN.

– Ataki na protokoły routingu.

– Mapowanie sieci.

– Skanowanie IP.

– Fingerprinting usług sieciowych i systemów.

Procedury użytkownika

- **Struktura standardu:**

• Wymagania audytu – wymagania testów technicznych:
  • Weryfikacja wykorzystanych usług zarządzających urządzeniami o znanych podatnościach np.: SNMP, SSH, Telnet, HTTP.
  • Sprawdzenie protokołu Discovery Protocol (CDP in case of Cisco).
  • Banner grabbing.
  • Test Content Addressable Memory (CAM) Security.
  • Test Port broadcast-storm control.
  • Test VLAN Hopping Attacks by switch spoofing.
  • Test VLAN Hopping attacks by double encapsulation.
  • L2 proxy attacks.
  • Private VLAN hopping.
  • Spanning Tree Attacks.
  • DHCP “Starvation”.