Dostępne zabezpieczenia w systemie SAP. Ochrona danych i ich zbiorów.

1. Dostęp użytkowników do systemu SAP ECC 6.0 RiL

Dostęp do zasobów systemu SAP ECC 6.0 RiL jest zabezpieczony poprzez trzy poziomy uwierzytelniania użytkownika systemu:

1. Poziom domeny systemu operacyjnego Windows.
2. Poziom VPN – dostęp i autoryzacja w oparciu o rozwiązanie Pulse Secure.
3. Poziom systemu SAP (dostęp poprzez klienta systemu SAP – SAP GUI).
4. Uprawnienia w systemie SAP ECC 6.00.

Rodzaje dostępu do:

1. Dla użytkownika końcowego poprzez klienta SAP:
   a. SAP GUI – aplikacja kliencka, za pomocą której użytkownik może się logować bezpośrednio do systemu SAP, w którym ma konto.
2. Dla administratorów systemu SAP poprzez:
   a. SAP GUI – aplikacja kliencka, za pomocą której użytkownik może się logować bezpośrednio do systemu SAP, w którym ma konto,
   b. przeglądarkę WWW – przeglądarka internetowa np. Internet Explorer,
   c. dostęp terminalowy – dostęp do systemu operacyjnego.
   Dostęp poprzez terminal zarezerwowany jest wyłącznie dla administratorów systemu SAP ECC 6.0 RiL oraz do ewentualnej wymiany plików z systemami zewnętrznymi.

1.1. Dostęp użytkowników końcowych

Dostęp użytkowników końcowych do systemu SAP może być realizowany wyłącznie za pomocą aplikacji klienckiej SAP Gui. Każdy z użytkowników systemu SAP ECC 6.0 RiL posiada własne, unikalne konto w systemie zabezpieczone hasłem dostępu.

W celu właściwej ochrony haseł przed niepowołanym dostępem do zasobów systemu produkcyjnego zostały wdrożone następujące reguły budowy haseł:

a. hasło musi składać się z minimum 9 znaków,
b. hasło musi zawierać przynajmniej 1 małą literę (od a do z),
c. hasło musi zawierać przynajmniej 1 dużą literę (od A do Z),
d. hasło musi zawierać przynajmniej 1 cyfrę (od 0 do 9),
e. hasło musi zawierać przynajmniej 1 znak specjalny (np. !@#$%&* itp.),
f. hasło nie może zawierać polskich znaków diakrytycznych (np. ą, ę).

Dodatkowe wymagania zabezpieczające:

a. hasło nie może zawierać kolejno dwóch identycznych znaków,
b. powtarzających się sekwencji znaków,
c. hasło nie może być identyczne z nazwą konta lub jego częścią,
d. hasło nie może być imieniem, nazwiskiem, datą urodzenia,
e. hasło wymaga zmiany maksymalnie co 30 dni,
f. minimalny okres pomiędzy kolejnymi zmianami hasła przez użytkownika to 2 dni,
g. hasło użytkownika musi być inne niż 5 ostatnio wprowadzonych haseł,
h. hasło nie może zawierać nazwy konta,
i. hasło musi składać się z co najmniej 5 różnych znaków,
j. hasło musi różnić się od poprzedniego co najmniej 3 znakami.

W celu dodatkowego ograniczenia możliwości nieuprawnionego dostępu wdrożone zostały poniżej wymienione reguły:

a. Sesja z systemem SAP jest automatycznie zrywana po 3 kolejnych nieudanych próbach zalogowania.
b. System SAP blokuje konto użytkownika po 5 nieudanych próbach zalogowania (błędne hasło). Odblokowanie jest możliwe jedynie poprzez uprawnione do tego osoby. Wniosek o odblokowanie konta musi być zarejestrowany w ITSM i realizowany zgodnie z procedurą odblokowywania konta.
c. System nie pozwala na wielokrotne logowanie tego samego użytkownika w tym samym czasie i do tego samego klienta (mandanta).
d. Administratorzy systemu SAP weryfikują logi nieudanych prób logowania w celu wykrycia niepowołanych prób dostępu.

1.2. Dostęp administratorów systemu

Administracja systemem SAP jest realizowana z poziomu:

1. Systemu operacyjnego:
   Dostęp realizowany jest poprzez konto systemowe administracyjne [SID]ADM zabezpieczone hasłem na poziomie systemu operacyjnego. Dostęp do niego posiadają administratorzy uprawnieni do wykonywania zadań administracyjnych z poziomu systemu operacyjnego.
2. Bazy danych:
   Dostęp realizowany jest poprzez:
   a. Konto systemowe administracyjne DB2[SID] zabezpieczone hasłem na poziomie systemu operacyjnego. Dostęp do niego posiadają administratorzy uprawnieni do wykonywania zadań administracyjnych dotyczących bazy danych z poziomu systemu operacyjnego.
   b. DBA COCKPIT narzędzie, które jest wykorzystywane do monitorowania i zarządzania bazą danych (poprzez interfejs użytkownika GUI) dla wszystkich działań i które obejmuje wszystkie aspekty obsługi bazy danych. Dostęp do niego posiadają administratorzy uprawnieni do wykonywania zadań administracyjnych dotyczących bazy danych z poziomu Aplikacji SAP (poprzez specjalnie opracowaną rolę w SAP).
3. Aplikacji SAP:
   Dostęp realizowany jest poprzez indywidualne konto w systemie SAP zabezpieczone hasłem dostępu wg zasad z punktu 1.1. Uprawnienia jakie posiada każdy administrator są zgodne z regułą "każdemu tylko to co niezbędne" tzn. w zależności od zakresu kompetencji i odpowiedzialności, udostępniany jest dostęp do wybranych komponentów Basis systemu SAP.

Administracja poszczególnymi poziomami (system operacyjny, baza danych, aplikacja SAP) została podzielona na zespoły administratorów.

2. Mechanizmy dostępu opis techniczny

2.1. Zastosowanie technik VPN

Dostęp do środowiska SAP jest realizowany za pomocą VPN w oparciu o rozwiązanie Juniper Secure Access. Uwierzytelnianie użytkownika odbywa się w oparciu o hasła użytkowników z usługi katalogowej Active Directory.

Dostęp użytkowników do serwerów jest filtrowany w oparciu o docelowe adresy IP i porty TCP. Poszczególnym użytkownikom nadawane są uprawnienia wymagane jedynie dla pracy w konkretnych strumieniach SAP (np. RiL, ZKL), gdzie mają założone konto użytkownika. Uprawnienia nadawane są w oparciu o grupy w Active Directory.

Ruch jest w całości szyfrowany poprzez rodzinę protokołów IPSec lub SSL/TLS.

2.2. Dostęp użytkowników systemu do drukarek

Wydruki z systemu SAP ECC 6.0 RiL są realizowane w warstwie prezentacji Front-End Printing czyli poprzez domyślną drukarkę zdefiniowaną w systemie operacyjnym na stacji użytkownika końcowego.

3. Architektura systemu

Infrastruktura IT dla środowiska systemu SAP RiL oparta jest o dwa centra obliczeniowe. Centrum podstawowe zlokalizowane w CPD Warszawa ul. Marsa 95 oraz centrum zapasowe zlokalizowane w Morach k/Warszawy (zwane dalej CPD Mory). Infrastruktura systemu SAP RiL jest zintegrowana ze środowiskiem WAN, LAN, SAN, systemem zdalnego dostępu, szyfrowania, ścian ogniowych oraz systemem wykonywania kopii bezpieczeństwa i archiwizacji.

W CPD Warszawa pracują systemy produkcyjne oraz testowo-deweloperskie. W CPD Mory w przypadku awarii centrum podstawowego będą pracować wyłącznie systemy produkcyjne.

Serwery bazy danych i centralnych instancji SAP pracują w klastrze w oparciu o serwery IBM POWER 750, oprogramowanie klastrowe PowerHA oraz system operacyjny IBM AIX.

Macierz dyskowa IBM V7000 zawierająca 48 dysków SAS o pojemności 900GB 10k, 92 dysków SAS o pojemności 300GB 15k oraz 4 dyski SSD o pojemności 400 GB zapewnia wymaganą wydajność na poziomie 20 000 IOPS oraz pojemność około 30 TB. Replikacja macierzowa odbywa się w trybie asynchronicznym.

Środowisko serwerów dialogowych zrealizowano w oparciu o serwery w technologii x86 (IBM HS22) w oparciu o system operacyjny Linux przy zastosowaniu mechanizmu wirtualizacji VMware vSphere.

Serwery dialogowe dla każdej instancji rozdzielone są pomiędzy dwie obudowy IBM BladeCenter H co zapewnia pełną ich redundancję w podstawowym CPD. W zapasowym CPD zastosowano jedną obudowę IBM BladeCenter H i serwery IBM HS22.

Wsparcie techniczne dla elementów infrastruktury jest na poziomie na poziomie 24/7 NBD (next business day).

4. Kopie bezpieczeństwa

Realizacja kopii bezpieczeństwa systemu SAP RiL oparta jest na wykorzystaniu oprogramowania EMC Networker i urządzenia składowania danych EMC Data Domain. System wykonywania kopii bezpieczeństwa replikuje skopiowane dane do drugiego urządzenia EMC DataDomain znajdującego się w innej serwerowni.

Raz dziennie wykonywana jest kopia baz danych (online) i systemów plików z czasem ochrony 1 miesiąc. W każdy ostatni piątek miesiąca jest wykonywana kopia miesięczna z czasem ochrony 1 rok. Dodatkowo w ciągu dnia wykonywane są kopie generowanych przez bazy danych redo-logów wyzwalane automatycznie przez bazę danych.

5. Koncepcja uprawnień w systemie mySAP.com

5.1. Zasady budowy uprawnień

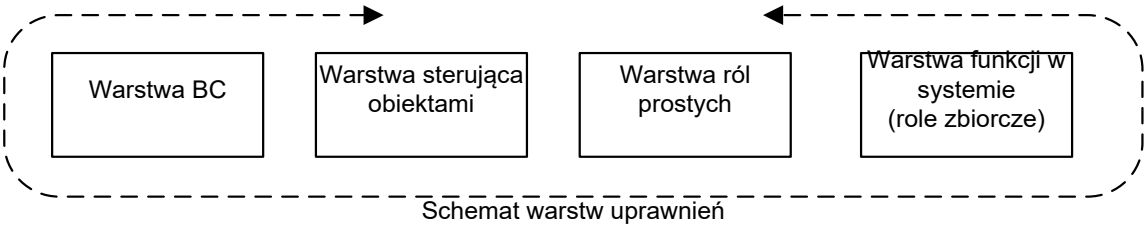
Koncepcja uprawnień w SAP ECC 6.00 pozwala na przydział ogólnych uprawnień użytkowników oraz szczegółowe określanie uprawnień danych użytkowników. Mogą one zostać ustalone na poziomie transakcji, pól oraz wartości. Większość uprawnień użytkowników daje prawa do obsługi poszczególnych obiektów SAP, ale mogą się one również odnosić do specyficznych operacji.

W celu ułatwienia administracji i przydzielania ról w systemie założono unifikację schematu budowy uprawnień we wszystkich modułach SAP bez względu na obsługiwane funkcjonalności. W tym celu przyjęto następujące założenia:

1. Oddzielenie menu użytkowników (**transakcje**) od profili uprawnień (**obiekty sterujące**).
2. Uproszczenie pojedynczych profili uprawnień (role pojedyncze to klocki do składania uprawnień dla poszczególnych użytkowników).
3. Wyodrębnienie grup użytkowników o podobnych zakresach zadań i uprawnień (Funkcje).
4. Wydzielenie stałych elementów uprawnień i zawarcie ich w odrębnych rolach pojedynczych (role sterujące).
5. Zachowanie zasady przyrostu uprawnień, gdzie role z ograniczonymi przywilejami wchodzą w skład ról z szerszymi uprawnieniami.
6. Zachowanie zasady nie dublowania transakcji w rolach (jedna transakcja występuje tylko w jednej roli).
7. Stworzenie odrębnego dokumentu koncepcji funkcjonowania uprawnień.
8. Ustalenie procedur dokonywania zmian w uprawnieniach.
9. Ustalenie ścisłej konwencji nazewnictwa.
10. Prowadzenie dokumentacji technicznej.
11. Wprowadzenie elektronicznego wnioskowania o uprawnienia (w obrębie RiL i BW).

5.2. Warstwy uprawnień

Koncepcja zakłada budowanie uprawnień użytkowników opartych na czterech warstwach czyli ról różnego rodzaju.



Schemat warstw uprawnień

5.2.1. Warstwa BC

Pierwszą warstwę stanowią role złożone z transakcji oraz obiektów uprawnień powszechnych dla wszystkich użytkowników (np. dostęp do poczty SAP, uprawnienia do drukowania dokumentów, transakcji SU53 itp.). Role z tej warstwy przydzielane są obligatoryjnie wszystkim użytkownikom systemu.

5.2.2. Warstwa sterująca obiektami – Role Sterujące

Warstwa sterująca obejmuje role zawierające transakcje oraz obiekty uprawnień zapewniające dostęp do elementów organizacyjnych bądź funkcjonalnych takich jak np. Jednostka Gospodarcza, Dział gospodarczy, Zakład, Konta KG itp.:

1. Role z tej warstwy przydzielane są zgodnie z procedurą przydzielania uprawnień.
2. Za tworzenie oraz zmiany ról odpowiadają Administratorzy poszczególnych zespołów.
3. Nadzór nad rolami prowadzi Zespół Ds. Uprawnień.
4. Role z tej warstwy przydzielane są zgodnie z procedurą przydzielania uprawnień.

5.2.3. Warstwa Ról Prostych

Warstwa obejmuje zbiór transakcji określonych przez obszar merytoryczny, które umożliwiają dostęp użytkownikom końcowym do określonych czynności w systemie. W skład tej warstwy wchodzą role modułowe, role międzymodułowe i role sterujące:

1. Role z tej warstwy wchodzą w skład ról zbiorczych czyli Funkcji.
2. Role z tej warstwy przydzielane są zgodnie z procedurą przydzielania uprawnień.
3. Za tworzenie oraz zmiany ról odpowiadają Administratorzy poszczególnych zespołów.
4. Nadzór nad rolami prowadzi Zespół Ds. Uprawnień.

5.2.4. Warstwa Funkcji w Systemie

Warstwa stanowi role zbiorcze przypisane użytkownikom zgodnie z pełnioną funkcją (stanowiskiem). Jest to podstawowy element ról przydzielanych użytkownikom:

1. Każda funkcja składa się z „n" ról prostych.
2. Nie następuje dublowanie funkcji ze względu na strukturę organizacyjną.
3. Każdy użytkownik pełniący określone obowiązki w spółce otrzymuje funkcję odpowiadającą czynnościom, które wykonuje.
4. Nie tworzy się funkcji przypisanych personalnie do poszczególnych osób (np. nie przypisuje się poszczególnym użytkownikom jedynie transakcji, których używają).
5. Funkcje muszą być zgodne z Koncepcja Biznesową Wzorca poszczególnych modułów.
6. Zawartość funkcji zweryfikowały poszczególne ZW.
7. Role z tej warstwy przydzielane są zgodnie z procedurą przydzielania uprawnień.

5.3. Obiekty kontrolne w programach i raportach klienckich

Wszelkie rozszerzenia klienckie tj. programy, raporty posiadają funkcję autoryzacji dostępu poprzez obiekty uprawnień zgodnie z rozdziałem „Obiekty wyłączone z ról" odpowiednio do zakresu funkcjonalnego rozszerzenia, modułu oraz wykorzystanych tabel.

Minimalny zakres autoryzacji:

1. Jednostka gospodarcza,
2. Dział gospodarczy,
3. MPK,
4. Zakład.

6. Bezpieczeństwo systemu

6.1. Okresowy przegląd uprawnień użytkowników

Zgodnie ze stosowaną Ogólną Koncepcją Uprawnień co najmniej raz do roku zaleca się:

- Porównanie ról w systemie z Koncepcją Uprawnień.
- Porównanie ról w systemie z rolami wnioskowanymi.
- Dostosowanie Koncepcji Uprawnień do aktualnych wymogów biznesowych.
- Okresowy przegląd polityk i procedur pod kątem ich aktualności i zgodności z celami biznesowym.

6.2. Przegląd ról pod kątem bezpieczeństwa

Co najmniej 2 razy w roku Zespół ds. Uprawnień dokonuje przeglądu ról pod względem bezpieczeństwa sprawdzając, przeprowadzając w szczególności:

1. Analizę ról pod kątem występowania niebezpiecznych obiektów uprawnień (S*).

Analiza dokonywana jest na podstawie raportu S_BCE_68002111 Użytkownicy lub role z kombinacjami krytycznych uprawnień. W przypadku stwierdzenia występowania obiektów niezgodnych z Koncepcją Uprawnień dokonywane są odpowiednie zmiany we wskazanych rolach.

2. Weryfikację uprawnień użytkowników pod kątem zajmowanych stanowisk.

Weryfikacja dokonywana jest poprzez przesłanie drogą elektroniczną do Koordynatorów ds. Uprawnień poszczególnych spółek list z uprawnieniami użytkowników. Koordynatorzy w porozumieniu z Właścicielami biznesowymi potwierdzają zwrotnie ich poprawność. W przypadku wystąpienia konieczności dokonania zmian zgłoszenie ich następuje standardową ścieżką. Każdy Koordynator ds. Uprawnień w spółce posiada dostęp do raportu ZCA_R_PFCG_CHECK_KUP - Wyświetlenie danych użytkowników, który umożliwia przegląd przypisanych uprawnień użytkowników dla danej spółki. Raport ten może być wykorzystany do w/w weryfikacji.

3. Weryfikację uprawnień użytkowników pod kątem ADP (Administracja Danych Podstawowych).

Weryfikacja dokonywana jest poprzez przesłanie drogą elektroniczną do osób odpowiedzialnych w GK PGE S.A. za zarządzanie danymi podstawowymi list z uprawnieniami ADP użytkowników. Osoby te potwierdzają zwrotnie ich poprawność. W przypadku wystąpienia konieczności dokonania zmian zgłoszenie ich następuje standardową ścieżką.

4. Weryfikację użytkowników pod kątem aktywności.

Weryfikacja dokonywana jest poprzez przesłanie automatycznie drogą elektroniczną raz w miesiącu do Koordynatorów ds. Uprawnień poszczególnych spółek list nie aktywnych użytkowników przez ostatnie 30 dni.

Raz na miesiąc dokonywana jest również weryfikacja aktywności użytkowników nie logujących się przez ostatnie 60 dni. W przypadku takich osób Zespół ds. Uprawnień dokonuje blokady użytkowników o czym informuje Koordynatorów ds. Uprawnień poszczególnych spółek.

5. Kontrolę poprawności realizacji zgłoszeń o zmianę uprawnień.

W odstępach kwartalnych Zespół ds. Uprawnień dokonuje kontroli losowo wybranych 10% lub nie więcej niż 20 zgłoszeń o nadanie uprawnień w celu weryfikacji czy uprawnienia faktycznie nadane w systemach SAP RiL są zgodne z wnioskowanymi.

7. Historia zmian danych – logi systemowe

Log systemowy systemu SAP jest plikiem zawierającym wszystkie zdarzenia, ostrzeżenia, błędy i inne informacje systemowe. Standardowo w logu systemowym rejestruje się wszystkie wyjątkowe zdarzenia systemu np. próby przekroczenia uprawnień, błędy zapisu w bazach danych, problemy systemowe itp. Ponadto wpisywane są informacje statystyczne, które pozwalają na kontrolę pracy systemu. Każdy zapis w logu zawiera pełną informację umożliwiają identyfikację zdarzeń.

Log audytu bezpieczeństwa służy do rejestrowania informacji związanych z bezpieczeństwem systemu. W logu audytu rejestrowane są zdarzenia takie jak:

1. Udane i nieudane próby logowania dialogowego.
2. Udane i nieudane próby logowania RFC.
3. Wywołanie funkcji RFC.
4. Uruchamianie transakcji, raportów.
5. Zmiana danych podstawowych użytkownika.
6. Zdarzenia systemowe.
7. Pozostałe zdarzenia.

Pliki logu audytu znajdują się na poszczególnych serwerach aplikacji i są przechowywane do momentu ich usunięcia (zarchiwizowania) przez administratora systemu.

Dodatkowo istnieje możliwość włączenia śledzenie systemu (tzw. trace): SQL trace, Enque trace, RFC trace. Wówczas możliwe jest śledzenie bardzo szczegółowych działań w systemie np.:

1. Wykonanie danych transakcji R/3.
2. Uruchomienie programów.
3. Odczytanie określonych dokumentów.
4. Zmiana pola danych (i to powyżej ustalonego zakresu).

Uruchomienie śledzenia musi być zaplanowane z uwzględnieniem zakresu potrzebnych informacji oraz wynikającego z uruchomienia śledzenia, znacznego obciążenia systemu (zmniejszenia wydajności oraz zwiększenia zajętości dysków).

8. Historia zmian danych – śledzenie zmian w dokumentach

Wszystkie zmiany danych transakcyjnych mogą być zapisywane w dziennikach (dokumentach) zmian na poziomie obiektów SAP ECC 6.0 RiL w poszczególnych modułach. Dokumenty zmian zawierają najczęściej informacje o:

1. Dacie wykonania zmiany.
2. Użytkowniku wykonującym zmianę.
3. Zawartości pola przed i po zmianie (dotyczy głównie danych podstawowych).

Dodatkowo każda operacja typu utworzenie lub zmiana dokumentu w systemie SAP jest opatrzona informacją, który użytkownik i kiedy je wykonał. Informacja ta jest przechowywana w ramach tzw. nagłówka dokumentu.

9. Zasady retencji danych

Zasady retencji danych określone są w PROG 00003 Procedura Ogólna wprowadzania i zmian danych Kontrahentów w systemie SAP RiL.