POLITYKA BACKUPU

W CELU ZMINIMALIZOWANIA RYZYKA UTRATY DANYCH W RAZIE AWARII,
DLA ZACHOWANIA CIĄGŁOŚCI DZIAŁANIA ORAZ REALIZACJI ZALECEŃ
Z ANALIZY RYZYKA ADMINISTRATOR SYSTEMÓW
INFORMATYCZNYCH WRAZ Z PRZESZKOLONYMI PRACOWNIKAMI
ZOBLIGOWANY JEST DO
WYKONYWANIA CODZIENNEGO BACKUPU DANYCH
WG OPRACOWANEGO SCHEMATU

Poniżej opisujemy te procesy oraz prezentujemy zalecenia do backupu, wskazując jak powinna wyglądać polityka backupu w Banku i na co należy zwrócić szczególną uwagę.

ZALECENIA DO POLITYKI BACKUPU

Polityka backupu powinna być ujęta w analizie ryzyka, jako jeden z ważniejszych elementów eksploatacji całego systemu Banku. To przecież pełnowartościowy backup ma zapewnić przywrócenie danych w razie braku stabilności podstawowego systemu i zachowanie ciągłości działania Banku w razie utraty stabilności podstawowego systemu bankowego.

Szczególnie zalecamy:

- Wykonywanie **codziennie kopii bezpieczeństwa** oraz ich zdublowanie
- Kopie bezpieczeństwa powinny być wykonywane na **trwałych nośnikach magnetycznych** – tu należy zdecydowanie podkreślić, że używane powszechnie klucze USB nie służą do przechowywania backupów, a jedynie mogą służyć do chwilowego magazynowania danych lub ich przenoszenia.

Servus Comp Sp. z o.o. Sp. K.
30-019 Kraków ul. Mazowiecka 25/502
tel. 12 631-91-22 biuro@servus-comp.pl
www.premiumbank.zadbajobezpieczenstwo.pl

- W miarę możliwości powinna się odbywać **cykliczna weryfikacja stwierdzająca poprawność wykonanych kopii** – plików. Może się zdarzyć tak, że urządzenie potwierdza wykonanie kopii, ale ta kopia jest uszkodzona i w razie konieczności nie będzie można z niej uruchomić potrzebnych plików
- Zalecamy np. **raz na kwartał lub raz na pół roku (im częściej tym lepiej) sprawdzanie poprawności wykonanych kopii** przez próbne uruchomienie skopiowanego pliku. Najlepszym modelem byłoby, żeby plik był uruchomiony w środowisku testowym na faktycznym systemie.
- **Należy** prowadzić **elektroniczny lub papierowy rejestr**, w którym operator potwierdza wykonanie czynności backupu. Potwierdzenie powinno zawierać: opisanie czynności, wielkość pliku, który powstał po wykonaniu backupu, datę i godzinę wykonania oraz potwierdzenie wykonania czynności własnoręcznym podpisem operatora wykonującego backup. Dodatkowo w Banku powinny być wyznaczone osoby uprawnione do wykonywania backupu.
- Kopie repozytoriów powinny być **wykonywane cykliczne** i backupowane do znanej nam lokalizacji. Ma to ogromne znaczenie, bo w razie uszkodzenia oprogramowania zarządzającego danym urządzeniem, w każdej chwili możemy wgrać ustawienie z kopii bezpieczeństwa.

W Bankach Spółdzielczych w Polsce dominującymi dostawcami głównych systemów Bankowych są trzy firmy:

- Firma SoftNet z Krakowa
- Firma NOVUM z Łomży
- Asecco Polska z Rzeszowa

Głównym celem backupu w tych systemach jest pełne bezpieczeństwo baz danych i zapewnienie użytkownikowi takiego backupu, który w razie utraty danych – utraty stabilności zapewni przywrócenie pełnej funkcjonalności. Wymienieni dostawcy systemów zapewniają narzędzia do wykonywania backupów.

Jeżeli standardowy backup nie jest dla nas optymalnym rozwiązaniem,
to warto określić:

RTO – Recovery Time Objective

czas potrzebny na odtworzenie danych po awarii do momentu przywrócenia pełnej funkcjonalności.

RPO - Recovery Point Objective

określa na jak dużą ilość danych utraconych możemy sobie pozwolić
oczekując na przywrócenie pełnej funkcjonalności systemu. Określa on występowanie rozbieżności sprzed awarii i po uruchomieniu systemu po awarii. Często, po uruchomieniu systemu po awarii sporządzana jest lista rozbieżności, która dokładnie określa, które dane zostały utracone.

Jeżeli analiza ryzyka, w której mamy określone wartości RPO i RTO wymaga od nas szybszego działania odnośnie przywrócenia system do pracy, to wtedy musimy zastanowić się nad wdrożeniem narzędzi,

servus comp
Servus Comp Sp. z o.o. Sp. K.
30-019 Kraków ul. Mazowiecka 25/502
tel. 12 631-91-22 biuro@servus-comp.pl
www.premiumbank.zadbajobezpieczenstwo.pl

które oprócz standardowego backupu będą wykonywały replikacje danych w czasie rzeczywistym lub w czasie, w którym ryzyko utraty danych będzie minimalne. Odzyskanie stabilnej pracy osiągniemy szybciej, jeżeli w systemie w czasie rzeczywistym lub zbliżonym do rzeczywistego wykonywana jest replikacja. Przywrócenie systemu z backupu wymaga dłuższego przestoju systemu bankowego, w czasie którego ten system jest przywracany.

PRZYKŁADOWY UNIWERSALNY SCHEMAT – POLITYKA BACKUPU	
Główny system Banku	Poniżej przykładowy schemat codziennego backupu: – główny system Bankowy w ciągu dnia pracy jest kopiowany co 30 minut na serwer kopii. Wykonywana kopia jest pełna. – w nocy wykonywana jest pełna kopia na serwer – dodatkowo kopiowane są wszystkie dane – po zamknięciu dnia księgowego wykonywana jest kopia – w systemie 1 nośnik na jeden dzień – kopię wykonuje ASI lub pracownik księgowości. Kopie umieszcza się w szafie pancernej, w specjalistycznej walizce do przechowywania kopii. – przed zakończeniem i po zakończeniu miesiąca wykonywane są kopie i po zatwierdzeniu poprawności zapisanych danych wykonywana jest kopia na DVD. Kopia przechowywana jest w szafie pancernej w zamykanej półce. Płyty są opisywane. Stosowane są różne techniki wykonywania backupu w zależności od dostawcy systemu bankowego.
ASIST	– dział księgowości wykonuje kopie np. na SYNOLOGY w serwerowni, następnie plik kopiowany jest na DVD na koniec miesiąca księgowego przez ASI – 1 x miesiąc ASI wykonuje kopię na płytę DVD na koniec miesiąca księgowego
PŁATNIK – KADRY – PŁACE	– pracownik odpowiedzialny za prowadzenie danych czynności jest odpowiedzialny za wykonanie kopii, którą wykonuje i składuje np. na SYNOLOGY na przydzielony zasób dyskowy tego urządzenia, następnie ASI zbiera kopie z przydzielonych katalogów i kopiuje je na nośnik DVD, który następnie składowany jest w szafie pancernej w strefie dodatkowo zamykanej.
REPOZYTORIUM URZĄDZEŃ	– ASI wykonuje kopie do folderu „KOPIA” np. na SYNOLOGY. Kopie wykonywane są cyklicznie w określonych odstępach czasowych lub przed wykonaniem większych zmian lub prac w infrastrukturze informatycznej.

servus comp
Servus Comp Sp. z o.o. Sp. K.
30-019 Kraków ul. Mazowiecka 25/502
tel. 12 631-91-22 biuro@servus-comp.pl
www.premiumbank.zadbajobezpieczenstwo.pl

W celu zapewnienia wykonywania pełnowartościowego backupu, Bank powinien opracować system backupu z wyborem optymalnego oprogramowania służącego do ochrony danych, które automatyzuje tworzenie kopii zapasowych. Oprogramowanie powinno być zainstalowane na dedykowanym serwerze lub na dedykowanym środowisku wirtualnym serwera oraz na podłączonej do niego np. bibliotece taśmowej.

Oprogramowanie powinno mieć możliwość zapisywania danych na różnych nośnikach danych takich jak dyski twarde, karty flash, taśmy magnetyczne, nośniki CD, DVD, BlueRay.

Przy wyborze oprogramowania do backupu warto się zastanowić, czy powinno zapewnić nam ono również deduplikację, czyli wyeliminowanie powtarzających się części w zbiorze danych. Dzięki takiemu rozwiązaniu, tylko niepowtarzalne dane zapisywane są na nośniku danych, dzięki czemu zyskujemy oszczędność ilości zajętego miejsca przez backup.

Program do backupu powinien nam umożliwić:

- zarządzanie backupami poprzez bazę danych zawierającą dane o kopiach zapasowych
- zarządzanie oprogramowaniem powinno odbywać się przez jego konsolę
- ustawienia konfiguracji klienta, polityki, harmonogramów monitorowania, raportów i codziennych operacji kopii zapasowych

Na rynku dostępne są różne systemy do backupu. W przypadku Banków Spółdzielczych dostawą optymalnego rozwiązania zwykle zajmuje się dostawca głównego systemu bankowego. Z reguły są to trafne wskazania.

W ramach wykonywania Testów Warunków Skrajnych jednym z testów muszą być wykonywane następujące testy stwierdzające poprawność wykonanych kopii:

- próbne odtworzenie danych z zautomatyzowanego procesu wykonanej kopii bezpieczeństwa. Kontrola ma na celu sprawdzenie czy kopiowane pliki nie są uszkodzone i będzie można w razie potrzeby odzyskać z nich dane.
- próbne uruchomienie środowiska zapasowego w oparciu o wykonane kopie systemu bankowego. Test wykonuje się zwykle w środowisku testowym symulującym realny system. Ma on na celu określenie czy w razie uszkodzenia lub utraty stabilności głównego systemu lub infrastruktury zarządzającej tym środowiskiem, będzie można przepiąć Bank na środowisko zastępcze, z którego dzięki wykonywanym codziennym kopiom, system będzie pracował na realnych danych systemu bankowego.

W celu uzyskania pełnej informacji w omawianych zakresach zapraszamy do kontaktu:

Andrzej Popiołek
Audytor Wiodący SZBI, Członek IIA Polska
+48 602 220 749 andrzej.popiolek@servus-comp.pl

Servus Comp Sp. z o.o. Sp. K.
30-019 Kraków ul. Mazowiecka 25/502
tel. 12 631-91-22 biuro@servus-comp.pl
www.premiumbank.zadbajobezpieczenstwo.pl

Ewa Niesiołowska
Audytor Wiodący SZBI, Członek IIA Polska
+48 531 364 287 ewa.niesiolowska@servus-comp.pl

Anna Stręk
Audytor Wiodący SZBI, Członek IIA Polska
+48 781 555 025 anna.strek@servus-comp.pl

Anna Kramarczyk
Kierownik ds. projektów IT
+48 794 671 787 anna.kramarczyk@servus-comp.pl

Servus Comp Sp. z o.o. Sp.k.
ul. Mazowiecka 25/502, 30-019 Kraków
Sąd Rejonowy dla Krakowa – Śródmieście,
XI Wydział Gospodarczy Krajowego Rejestru Sądowego
NIP: 6772394344 | Regon: 362815411 | KRS: 0000582481
https://zadbajobezpieczenstwo.pl
https://premiumbank.zadbajobezpieczenstwo.pl