INFORMATYKA EKONOMICZNA BUSINESS INFORMATICS 2(40) • 2016

ISSN 1507-3858
e-ISSN 2450-0003

Artur Rot
Uniwersytet Ekonomiczny we Wrocławiu
e-mail: artur.rot@ue.wroc.pl

Mateusz Pękala
ActIT
e-mail: mateusz.pekala@actit.pl

TWORZENIE KOPII ZAPASOWYCH I ODZYSKIWANIE DANYCH JAKO ELEMENT SYSTEMU ZARZĄDZANIA CIĄGŁOŚCIĄ DZIAŁANIA ORGANIZACJI

BACKUP AND DATA RECOVERY AS AN ELEMENT OF BUSINESS CONTINUITY MANAGEMENT SYSTEM IN THE ORGANISATION

DOI: 10.15611/ie.2016.2.07
JEL Classification: O30, O32

Streszczenie: Zarządzanie ciągłością działania (BCM – *Business Continuity Management*) polega na opracowaniu rozwiązań i procedur umożliwiających takie działanie w sytuacji kryzysowej, które pozwoli na utrzymanie funkcjonowania najważniejszych procesów biznesowych w organizacji na minimalnym akceptowalnym poziomie. Rozwiązania te są ściśle związane z zapewnieniem nieprzerwanych działań na płaszczyźnie IT. Niniejszy artykuł przybliża tematykę zarządzania ciągłością działania, planu odzyskiwania utraconych zasobów (DRP – *Disaster Recovery Plan*) czy też szerzej – planu ciągłości działania (BCP – *Business Continuity Plan*). Jako podstawowe narzędzia DRP wskazano system tworzenia kopii zapasowych i odzyskiwania danych. Na przykładzie oprogramowania firmy Veeam Software scharakteryzowano działanie systemu backupowego w kontekście roli, jaką odgrywa w systemie zarządzania ciągłością działania organizacji, który z kolei należy traktować jako element systemu zarządzania bezpieczeństwem informacji.

Słowa kluczowe: bezpieczeństwo systemów informatycznych, zarządzanie ciągłością działania, plan ciągłości działania, plan odzyskiwania utraconych zasobów.

Summary: Business Continuity Management (BCM) is to develop solutions and procedures to enable action in a crisis situation, which will allow to maintain the functioning of key business processes at a minimum acceptable level. These solutions are closely related to ensuring the uninterrupted IT activities. This article introduces the subject of Business Continuity Management, Disaster Recovery Plan and Business Continuity Plan. Backup and recovery systems have been indicated as basic DRP tools. The aim of this article is also to characterize

the backup system in the context of its role in the Business Continuity Management System in the organization, which is part of the Information Security Management System in the information technologies area.

Keywords: IS security, Business Continuity Management, Business Continuity Plan, Disaster Recovery Plan.

1. Wstęp

Pod koniec XX wieku pojawiła się koncepcja zintegrowanego zarządzania ryzykiem w obszarze bezpieczeństwa systemów informatycznych, natomiast aktualnie podejście do zarządzania ryzykiem ewoluuje w stronę zapewnienia ciągłości działania [Monkiewicz 2010, s. 64]. Ciągłość działania, u podstaw której leży inżynierskie podejście do niezawodności procesów produkcyjnych, jest rozumiana jako postępowanie organizatorskie tworzące zdolność organizacji do skutecznego reagowania w sytuacji zaistnienia zakłócenia jako wyniku swoistej interakcji przejawów zagrożenia z podatnością organizacji wewnętrznej infrastruktury lub zasobów. W tym sensie zapewnianie ciągłości działania jest przedmiotem zarządzania operacyjnego i stanowi ostatnie ogniwo zarządzania ryzykiem operacyjnym.

Ogólnie ciągłość działania to zdolność organizacji do takiego reagowania na zakłócenia warunków normalnej działalności, aby tam, gdzie to możliwe, szybko przywrócić te normalne warunki, a tam, gdzie to niemożliwe, przejść do zaplanowanego sposobu zastępczego wykonywania zadań. Postrzega się ją zarówno w kontekście zadań organizacji oraz procesów służących realizacji tych zadań, jak i w kontekście czynników mogących zakłócić te procesy oraz podatności organizacji, stanowiącej o jej wrażliwości na zakłócenia [Staniec, Zawiła-Niedźwiecki 2015, s. 283]. Celem niniejszego artykułu jest przybliżenie zagadnień zarządzania ciągłością działania (BCM – *Business Continuity Management*), planu odzyskiwania utraconych zasobów (DRP – *Disaster Recovery Plan*) czy też planu ciągłości działania (BCP – *Business Continuity Plan*). Jednym z ważnych elementów tego systemu są rozwiązania służące do wykonywania kopii bezpieczeństwa i odzyskiwania danych. Jako podstawowe narzędzia DRP wskazano system tworzenia kopii zapasowych i odtwarzania danych. Na przykładzie oprogramowania firmy Veeam Software scharakteryzowano system backupu danych w kontekście roli, jaką odgrywa on w systemie BCM organizacji.

2. Zarządzanie ciągłością działania w organizacji

W ciągu ostatnich kilku lat w sposób zasadniczy zmieniło się podejście do utrzymania ciągłości trwania i działania przedsiębiorstwa. Kraje europejskie wykazują ogromne zainteresowanie ekonomicznym i operacyjnym zabezpieczeniem trwania organizacji [Rot 2016]. Zwraca się uwagę na odpowiedzialność przedsiębiorcy za

zapobieganie kryzysom i na rolę rządu jako gwaranta publicznego bezpieczeństwa [Kaczmarek, Ćwiek 2009, s. 30]. Istotną przesłanką stanowiącą o potrzebie odpowiedniego podejścia do problematyki zarządzania ciągłością działania są nie tylko wymogi wynikające z regulacji prawnych, ale przede wszystkim fakt, że kontrolowanie ryzyka i umiejętne planowanie ciągłości funkcjonowania organizacji wpływa pozytywnie na wartość organizacji, wizerunek i możliwość osiągania zaplanowanych celów.

Zarządzanie ciągłością działania to podejście do prowadzenia działalności gospodarczej w sposób pozwalający na utrzymanie określonego poziomu dostarczania produktów lub świadczenia usług w przypadku wystąpienia istotnych zakłóceń w funkcjonowaniu procesów organizacji. Ogólnie mówiąc, zarządzanie ciągłością działania polega na identyfikacji zagrożeń dla funkcjonowania organizacji i na opracowaniu sposobów postępowania w przypadku wystąpienia zdarzeń, które mogą zakłócić to funkcjonowanie (opracowanie planów awaryjnych, wdrożenie środków technicznych, zastosowanie zabezpieczeń informatycznych oraz rozwiązań organizacyjnych) [DGA 2016]. Efektem wdrożenia systemu zarządzania ciągłością działania powinien być m.in. odpowiedni plan ciągłości działania, określający zestaw procedur, przepisów, dokumentów, które będą wskazywać zasady postępowania w razie nieoczekiwanego wystąpienia zakłócenia normalnej działalności organizacji [Janas, Perłowski 2007].

Plany ciągłości działania są zatem bardzo ważnym elementem zarządzania ciągłością działania. Proces ten, wraz z planami ciągłości działania, powinien być obecny w każdej organizacji, w której jakikolwiek przestój może okazać się fatalny w skutkach, np. przez generowanie znacznych strat. Plany te identyfikują ścieżki dla poszczególnych systemów informatycznych, wskazują osoby odpowiedzialne za ich uruchomienie i realizację, zawierają opisy procedur, które muszą być wykonane, by przywrócić dostępność danych i możliwość funkcjonowania procesów (np. częstotliwość, sposoby i narzędzia archiwizacji itp.) [Janas, Perłowski 2007]. Ważną częścią planu ciągłości działania jest plan odzyskiwania utraconych zasobów, który składa się, ogólnie rzecz biorąc, z procedur postępowania w wypadku zdarzenia losowego lub krytycznej awarii, w wyniku której procesy w organizacji zostają przerwane, a zasoby i dane utracone.

3. Zarządzanie ciągłością działania a zarządzanie ryzykiem

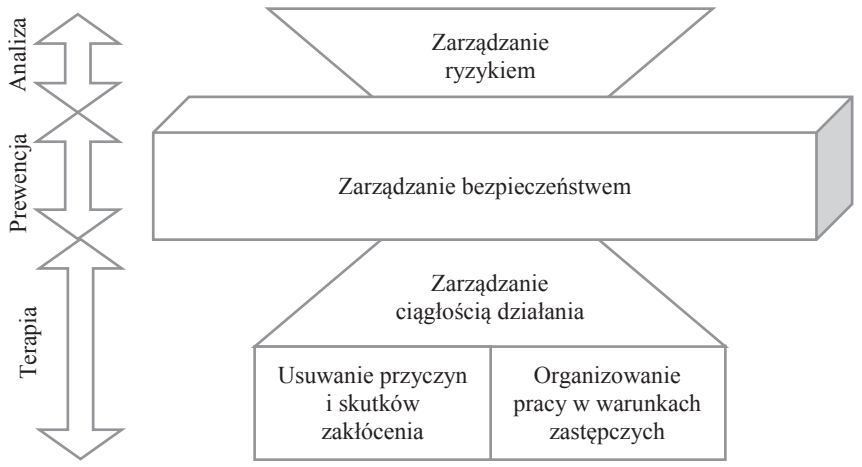
Zarządzanie ciągłością działania jest pojęciem dość nowym, bardzo mocno związanym z pojęciem zarządzania w ogóle, ale jednak najbliższym idei zarządzania ryzykiem. Nie jest jednak z nim tożsame i jako nowoczesne narzędzie zarządzania organizacją wspomagane jest przez zintegrowane i interdyscyplinarne zarządzanie ryzykiem [Kaczmarek, Ćwiek 2009, s. 30]. W tabeli 1 przedstawiono pewne różnice w podejściu do zarządzaniem ryzykiem i zarządzania ciągłością działania.

Tabela 1. Podejście do zarządzania ryzykiem oraz zarządzania ciągłością działania

Charakterystyka	Zarządzanie ryzykiem	Zarządzanie ciągłością działania
Główna metoda	Analiza ryzyka	Analiza ciężaru strat (*business impact analysis*)
Główne parametry	Zdarzenie i prawdopodobieństwo jego wystąpienia	Zdarzenie oraz czas jego wystąpienia i trwania
Rodzaj zdarzenia	Wszystkie typy – jednak możliwe do sklasyfikowania i nie zawsze wyraźnie wpływające na działalność	Różne rodzaje zdarzeń istotnie wpływające na zachwianie równowagi przedsiębiorstwa
Waga i rozmiar zdarzeń	Różne rozmiary – jednak koszty możliwe do oszacowania	Strategia zaplanowana do pokonania każdej trudności niezależnie od wagi zdarzenia
Zakres	Skupienie na ryzykach odnoszących się głównie do podstawowej działalności przedsiębiorstwa	Skupienie się przede wszystkim na wydarzeniach mających potencjalny lub realny wpływ na biznes – głównie poza podstawową działalnością organizacji
Siła i sposób oddziaływania	Od problemów narastających do nagłych incydentów	Głównie nagłe i szybkie wydarzenia; kultura UCD pozwalająca pokonać narastające problemy

Źródło: [Kaczmarek, Ćwiek 2009].

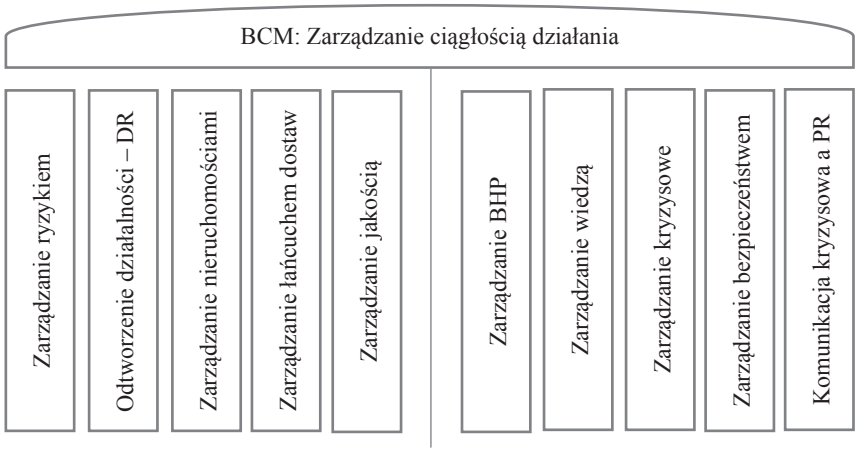
Dobrą ilustracją relacji między zarządzaniem ryzykiem a zarządzaniem ciągłością działania w szerszym kontekście zarządzania bezpieczeństwem organizacji jest rys. 1.



Rys. 1. Relacja zadań bezpieczeństwa i zapewnienia ciągłości działania

Źródło: [Staniec, Zawiła-Niedźwiecki 2008, s. 262].

Można stwierdzić, iż zarządzanie ciągłością działania jest holistycznym procesem zarządzania, który ma na celu określenie potencjalnego wpływu na organizację i stworzenie warunków budowania odporności na nie oraz zdolności skutecznej reakcji w zakresie ochrony kluczowych interesów właścicieli, reputacji i marki organizacji, a także wartości osiągniętych w dotychczasowej działalności [Wołowski, Zawiła-Niedźwiecki 2012, s. 285].



Rys. 2. Holistyczny proces zarządzania ciągłością działania

Źródło: [Wołowski, Zawiła-Niedźwiecki 2012, s. 285].

Właściciele procesów związanych z systemem zarządzania ciągłością działania w organizacji powinni współpracować na rzecz ciągłego doskonalenia tegoż procesu, stąd też często mówi się o potrzebie osadzenia BCM w kulturze organizacji.

4. Wybrane źródła dobrych praktyk przy tworzeniu systemu zarządzania ciągłością działania w organizacji

Utrwalonymi źródłami dobrych praktyk w zakresie zapewniania ciągłości działania są m.in. [Wołowski, Zawiła-Niedźwiecki 2012, s. 280]:

- dobrowolne w stosowaniu normy (ISO oraz narodowe) dotyczące zarządzania ryzykiem operacyjnym oraz zapewniania jakości lub bezpieczeństwa, które wskazują wytyczne zapewniania ciągłości działania,
- dobrowolne w stosowaniu normy (ISO oraz narodowe) dotyczące zapewniania ciągłości działania,
- rekomendacje branżowe dotyczące zarządzania kryzysowego i zapewniania bezpieczeństwa oraz ciągłości działania, zwłaszcza w bankowości (Rekomendacje Komitetu Bazylejskiego, tzw. *Basel II*) i ubezpieczeniach (Dyrektywa UE – *Solvency*),

- metody projektowania rozwiązań organizacyjnych oraz technicznych, w tym zwłaszcza informatycznych, uwzględniające wymogi zapewniania jakości, bezpieczeństwa i ciągłości działania.

Ciągłość działania jest przedmiotem wymagań stawianych przez przepisy Unii Europejskiej i poszczególnych jej krajów, zbiory rekomendacji branżowych oraz standardy międzynarodowe. Zapewnianie ciągłości działania początkowo traktowane było łącznie z problematyką bezpieczeństwa informacji, dlatego też przewija się wraz z tamtym zagadnieniem w serii norm ISO/IEC 27000 czy też standardzie ISO/IEC TR 13335.

Normy BS 25999 i BS 25777 autorstwa BSI przynoszą pożądaną standaryzację w zakresie BCM i mogą stanowić istotną pomoc dla organizacji wdrażających tego typu rozwiązania. BS 25999 to pierwsza na świecie brytyjska norma zarządzania ciągłością działania opracowana w celu zminimalizowania ryzyka takich incydentów [BSI 2016]. Seria standardów o symbolu BS 25999 została opracowana w 2007 r. przez BSI (British Standards Institution) – najstarszą na świecie instytucję zajmująca się tworzeniem norm i standardów, uznawaną za jedną z ważniejszych organizacji w zakresie normalizacji i certyfikacji. Wspomniana seria standardów dotyczy obszaru zarządzania ciągłością działania w organizacji i wprowadza systemowe podejście do tego zagadnienia w oparciu o dobre praktyki. BS 25999 został opracowany przez specjalistów, zarówno teoretyków, jak i praktyków z różnych krajów, na bazie badań akademickich, a także doświadczeń praktycznych w zarządzaniu ciągłością działania. Norma BS 25999 składa się z dwóch zasadniczych standardów. Pierwszy z nich, mający oznaczenie BS 25999–1, nosi pomocniczą nazwę *Code of Practice* (kodeks praktyk) i jest zbiorem wytycznych, które wprowadzają procesy, zasady, a przede wszystkim niezbędną terminologię [BS 25999–1: 2006; Kaczmarek, Ćwiek 2009, s. 37-38]. Druga norma o symbolu BS 25999–2 nosi nazwę *Specification for Business Continuity Management* (specyfikacja dla zarządzania ciągłością działania) i jest standardem określającym wymagania co do wdrożenia środków kontroli ciągłości działania, w oparciu o które może być przyznany certyfikat zgodności [BS 25999–2:2007; Kaczmarek, Ćwiek 2009, s. 38].

Pierwsza część normy o symbolu BS 25999–1:2006 koncentruje się na następujących kwestiach i problemach [BS 25999–1:2006]:

- polityka zarządzania ciągłością działania definiująca cele kierownictwa,
- proces zarządzania ciągłością funkcjonowania organizacji zapewniający systemowe podejście,
- analiza działalności przez pryzmat ryzyka,
- strategia zarządzania ciągłością działania jako odpowiedź na istniejące rodzaje ryzyka,
- opracowanie i wdrożenie środków ochrony (m.in. BCP, DRP) wynikających z realizacji strategii,
- testowanie, zarządzanie i przegląd środków ochrony – zarówno technicznych, jak i organizacyjnych (przede wszystkim planów awaryjnych),
- budowa świadomości pracowników i podmiotów współpracujących z organizacją.

Natomiast druga część standardu opisana symbolem BS 25999–2:2007 porusza następujące obszary i zagadnienia [BS 25999–2:2007]:

- terminy i definicje,
- planowanie systemu zarządzania ciągłością biznesu (BCMS),
- wdrażanie i eksploatowanie systemu BCMS – standard charakteryzuje te procesy jako składające się z następujących działań:
  - poznanie organizacji,
  - analiza wpływu na działalność biznesową,
  - szacowanie ryzyka,
  - określanie opcji postępowania z ryzykiem,
  - określanie strategii ciągłości biznesu,
  - opracowywanie i wdrażanie odpowiedzi na zdarzenia BCM,
  - testowanie, utrzymywanie i przeglądanie planów ciągłości działania,
  - monitorowanie i przegląd systemu BCMS,
  - utrzymywanie i doskonalenie systemu BCMS.

Kolejna norma – BS 25777 wspomaga planowanie, organizację i wdrażanie strategii ciągłości funkcjonowania technologii informacyjno-komunikacyjnych (*Information and Communications Technologies* – ICT) w organizacji. Zarządzanie ciągłością działania ICT wspomaga ogólne zarządzanie procesami organizacji, zapewnia, że technologie informatyczne oraz usługi IT są elastyczne i mogą być odzyskane w terminach wymaganych i uzgodnionych z najwyższym kierownictwem. Skuteczne zarządzanie ciągłością działania zależy od ciągłości tych technologii, aby organizacja mogła osiągać swoje cele przez cały czas, szczególnie zaś w okresach zakłóceń.

5. Wybrane funkcjonalności systemu backupowego na przykładzie produktów Veeam Software

Wdrożenie systemu zarządzania ciągłością działania ma na celu zabezpieczenie organizacji m.in. przed utratą cennych danych, a dzięki temu – przed ryzykiem wstrzymania działalności biznesowej. Jednym z ważnych elementów tego systemu są rozwiązania służące do wykonywania kopii bezpieczeństwa i odzyskiwania danych. Ich producenci dostrzegają, że ich oprogramowanie nie może funkcjonować w próżni i musi odpowiadać na potrzeby organizacji ujęte w ich systemie zarządzania ciągłością działania. Dobrym przykładem są rozwiązania firmy Veeam Software opisane poniżej. Wychodzą ona poza rolę standardowego backupu, oferując możliwość testowania poprawek, szkolenie pracowników i prowadzenie prac programistycznych, oferują również wsparcie w zakresie planowania DR.

Rosnąca wartość informacji wymaga zapewnienia odpowiedniej strategii zarządzania danymi, która powinna być nieodzowną częścią planów ciągłości działania organizacji. Optymalny wybór systemu zarządzania kopiami zapasowymi gwarantuje bezpieczeństwo danych oraz pewność szybkiego i niezawodnego odtworzenia danych. Budowa zintegrowanego systemu zarządzania danymi powinna uwzględ-

niać politykę archiwizacji danych organizacji. Archiwizacja rozwiązuje problemy rosnących kosztów utrzymania i zakupu drogich systemów dyskowych, konieczności rozbudowy systemów zarządzania kopiami zapasowymi, spełnienia wymogów prawnych związanych z przetwarzaniem danych. Zapasowe centra danych, replikacja danych, backup i archiwizacja danych, itp., mające na celu zwiększenie poziomu niezawodności i dostępności użytkowanych systemów informatycznych i minimalizujących ryzyko utraty zgromadzonych w nich danych – to główne elementy systemu zarządzania ciągłością działania. Poniżej scharakteryzowane zostaną wybrane narzędzia tego typu oferowane przez firmę Veeam Software.

Firma Veeam Software została założona w 2006 r. i od początku skupiała się na rozwiązaniach do zapewnienia ciągłości działania w nowoczesnych (zwirtualizowanych) centrach danych. W artykule omówione zostaną następujące rozwiązania Veeam Software, kładące duży nacisk na utylizację chmury prywatnej, publicznej i hybrydowej:

- Veeam Backup and Replication, który jest rozwiązaniem do backupu i replikacji dla środowisk wirtualnych VMware i Hyper-V,
- Veeam Availability Orchestrator, który koordynuje tworzenie kopii zapasowych i replik Veeam przez zdefiniowany plan DR, testy, które nie zakłócają pracy systemu oraz automatyczne dokumentowanie, aktualizowanie i raportowanie,
- Veeam One, stanowiący narzędzie komplementarne do produktu Veeam Backup and Replication służące do monitorowania backupu i samego środowiska wirtualnego.

5.1. Veeam Backup and Replication

Veeam Backup and Replication jest bezagentowym rozwiązaniem do backupu i replikacji dla środowisk wirtualnych VMware i Hyper-V. Jedną z najbardziej spektakularnych możliwości rozwiązania Veeam Backup and Replication jest funkcja **Instant VM Recovery**. Dzięki jej zastosowaniu możliwe jest uruchomienie maszyny wirtualnej bezpośrednio z pliku kopii zapasowej i tym samym bardzo szybkie (liczone w minutach) przywrócenie jej do działania. Jeżeli maszyna wirtualna ma dysk o pojemności kilku terabajtów, to możliwość natychmiastowego (liczonego w minutach) jej odzyskania bez potrzeby wielogodzinnego kopiowania wydaje się spektakularnie atrakcyjna. Wynikają z tego następujące korzyści [Veeam Software 2016d]:

- utrzymanie krótkich czasów odzyskiwania (niskiego poziomu RTO – *Recovery Time Object* – wskaźnik, który pozwala określić, jak długo będzie trwało odtwarzanie stanu bazy sprzed awarii systemu),
- ograniczenie przerw,
- ograniczenie przestojów maszyn wirtualnych o kluczowym znaczeniu.

Kolejną wartą odnotowania możliwością w Veeam Backup and Replication jest funkcjonalność **SureBackup**, czyli weryfikacja poprawności kopii zapasowych.

Opisana wyżej możliwość uruchomienia maszyny bezpośrednio z pliku backupowego (Instant VM Recovery) jest tutaj również wykorzystywana. Funkcja SureBackup umożliwia automatyczną weryfikację możliwości odzyskania danych z każdej kopii zapasowej każdej maszyny wirtualnej. Powoduje ona automatyczne uruchomienie maszyny wirtualnej w izolowanym środowisku Virtual Lab, wykonanie serii testów i wysłanie raportu na wskazany adres e-mail. W ten sposób administrator zyskuje pewność, że maszyny wirtualne będzie można w każdej chwili odzyskać.

Aby zweryfikować możliwość odzyskania danych z kopii zapasowej maszyny wirtualnej, funkcja SureBackup wykonuje następujące czynności:

- automatycznie uruchamia maszynę wirtualną w izolowanym środowisku bezpośrednio z pliku kopii zapasowej – trwa to o wiele godzin krócej niż pełne odzyskiwanie maszyny wirtualnej wykonywane przez konkurencyjne rozwiązania,
- wykonuje na maszynie wirtualnej serię testów, obejmujących np. funkcje sieciowe i status aplikacji,
- wyłącza maszynę wirtualną,
- tworzy raport o stanie kopii zapasowej maszyny wirtualnej.

Cały dostęp do kopii zapasowej maszyny wirtualnej odbywa się z prawem tylko do odczytu, a po zakończeniu procesu wszelkie zmiany są odrzucane [Veeam Software 2016c].

Testowanie backupów jest dużym wyzwaniem dla organizacji. Brak infrastruktury testowej i czasochłonność konfiguracji testów powodują, że wiele organizacji (nawet mającej testy uwzględnione w procedurach) nie wykonuje ich lub wykonuje je rzadziej, niż powinna (lub, co gorsza, fikcyjnie). Natomiast odpowiednie przeprowadzenie tego procesu, a co więcej – jego pełna automatyzacja przynosi wiele korzyści.

Kolejna funkcjonalność rozwiązania – **Virtual Lab** (laboratorium wirtualne) jest realizacją idei, wykorzystania potencjału danych przechowywanych w formie backupu. Rozwiązanie Veeam Backup and Replication pozwala automatycznie utworzyć izolowane, a przy tym łatwo dostępne środowisko wirtualne na potrzeby odzyskiwania elementów aplikacji, weryfikowania kopii zapasowych i replik maszyn wirtualnych oraz prowadzenia testów, szkoleń i rozwiązywania problemów bez wpływu na środowisko systemu.

Technologia Virtual Lab umożliwia uruchamianie maszyn wirtualnych bezpośrednio z kopii zapasowej lub repliki w izolowanych środowisku wirtualnym – bez potrzeby alokowania dodatkowego miejsca w pamięci masowej czy hosta zapasowego [Veeam Software 2016b].

Izolowane środowisko, które jest kopią oprogramowania i danych firmy, przynosi organizacji wiele potencjalnych korzyści. Może zostać wykorzystane m.in. do [Veeam Software 2016b]:

- testowania rozwiązań problemów przed ich zastosowaniem w środowisku informatycznym firmy,
- unikania problemów z wdrażaniem dzięki testowaniu nowych aplikacji i konfiguracji,

- szkolenia pracowników na rzeczywistym środowisku IT i danych organizacji (bez faktycznego narażania rzeczywistych systemów i danych na wystąpienie błędów),
- testowania uaktualnień i poprawek aplikacji.

Wykorzystanie takiego wirtualnego laboratorium na żądanie umożliwia skuteczniejsze, prostsze i łatwiejsze realizowanie procedur bezpieczeństwa zawartych w polityce bezpieczeństwa organizacji.

5.2. Veeam One

Veeam One to narzędzie komplementarne do produktu Veeam Backup and Replication służące do monitorowania backupu i samego środowiska wirtualnego. Ciągłe monitorowanie i ulepszanie powinno być immanentną cechą procesu systemu zarządzania ciągłością działania. W taką filozofię znakomicie się wpisuje Veeam One, dostarczając administratorowi backupu i/lub środowiska wirtualnego pulpit *Morning Coffee* oraz raporty analityczne niezbędne do utrzymania dostępności nowoczesnego centrum danych. Veeam One jest narzędziem, które pozwala szybciej dostrzegać potencjalne problemy i reagować na nie, wdrażając plany naprawcze, zanim nastąpi problem i zagrożona zostanie ciągłość działania organizacji [Veeam Software 2016e].

5.3. Veeam Availability Orchestrator

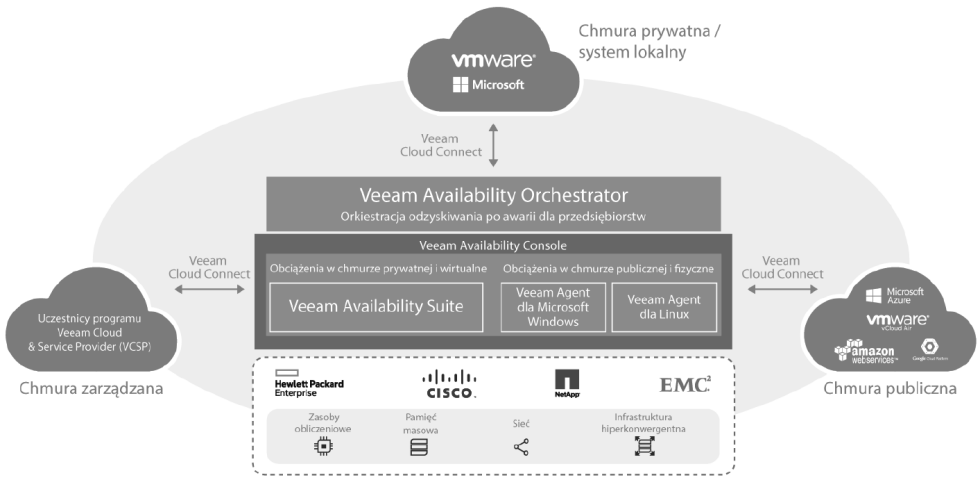
Veeam Availability Orchestrator jest nowym produktem firmy Veeam. Rozwiązanie to przez współpracę z rozwiązaniem Veeam Availability Suite i Veeam Backup & Replication ma za zadanie wspomóc organizację w realizacji założeń planu odzyskiwania utraconych zasobów (DRP) [Veeam Software 2016a].

Na rys. 3 zilustrowano umiejscowienie Veeam Availability Orchestrator w relacji do pozostałych rozwiązań producenta w zakresie zapewnienia dostępności danych.

Veeam Availability Orchestrator koordynuje tworzenie kopii zapasowych i replik Veeam przez zdefiniowany plan DR, testy, które nie zakłócają pracy systemu, oraz automatyczne dokumentowanie, aktualizowanie i raportowanie. Takie połączenie funkcji pomaga klientom korporacyjnym zagwarantować dostępność danych i aplikacji, zachować wysoki poziom niezawodności, ograniczyć koszty procesów sterowanych ręcznie i spełnić wymogi prawne [Veeam Software 2016a].

Veeam Availability Orchestrator umożliwia koordynację usuwania skutków awarii i współdziała z Veeam Availability Suite oraz Veeam Backup & Replication, przez co rozwiązuje obecne problemy z planami DR. Nowe rozwiązanie Veeam zostało zaprojektowane z myślą o przedsiębiorstwach i oferuje m.in. następujące funkcje [Veeam Software 2016a]:

- koordynacja – ścisła koordynacja kopii zapasowych i replik w ramach zdefiniowanego planu DR,



Rys. 3. Schemat rozwiązań Veeam zapewniających dostępność danych

Źródło: [Veeam Software 2016a].

- zautomatyzowane testy DR – automatyczne testy, które nie zakłócają działania systemu, pozwalające utrzymać wysoką niezawodność i uniknąć kosztownych, ręcznie sterowanych procesów,
- zgodność z przepisami i dokumentowanie – wbudowany system dokumentowania, aktualizowania i raportowania planów DR w celu spełnienia wymogów prawnych.

Według Gartner Group do 2020 r. 30% organizacji będzie wykorzystywać backup nie tylko do odtwarzania po awarii [Gartner... 2016]. Dane zgromadzone w backupie, poza swoją oczywistą funkcją, mogą być wykorzystane do DR, testów środowiska informatycznego i jego rozwoju, a także do prowadzenia prac programistycznych.

Na przykładzie produktów Veeam Backup and Replication omówiono, jak narzędzie backupowe wspomaga jednocześnie replikację danych i oferuje możliwość przełączenia awaryjnego. Rozwiązania Veeam idą dalej i w pakiecie Veeam Availability Orchestrator koordynują proces tworzenia kopii zapasowych i replik przez zdefiniowany plan DR, testowanie, które nie zakłócają pracy systemu oraz automatyczne dokumentowanie, aktualizowanie i raportowanie. Jest to kierunek, w którym będzie szło więcej producentów tego typu rozwiązań do wykonywania kopii zapasowych.

Kolejną bardzo pożądaną funkcjonalnością procesu utrzymania ciągłości działania jest możliwość testowania poprawek, dużych uaktualnień oprogramowania i systemów używanych przez organizację. Opisana funkcjonalność, nazywana przez firmę Veeam Software „Virtual Lab", pozwala na uruchomienie maszyn bezpośrednio z backupu w odizolowanym wirtualnym środowisku. W ten sposób uzyskujemy,

bliźniacze do naszego, działające środowisko informatyczne, na którym wykonujemy pożądane aktualizacje i inne działania konserwujące.

6. Zakończenie

Zmiany w nowoczesnych *data center* (wirtualizacja, nowoczesne macierze dyskowe, *cloud computing*) otworzyły ogromne możliwości w obszarze zapewnienia ciągłości działania. Zaczęto nawet stawiać tezy, że DR to już archaizm w dobie klastrów wysokiej dostępności, rozproszonych geograficznie centrów przetwarzania danych, w których replikacja pojedynczych transakcji bazodanowych odbywa się w czasie rzeczywistym. W takich warunkach nawet kompletna katastrofa z punktu widzenia użytkownika może oznaczać zaledwie chwilowe spowolnienie usługi.

Jednakże wszystkie te rozwiązania, pomimo ogromnej odporności, nie gwarantują 100% zabezpieczenia. Nie można całkowicie wyeliminować ryzyka, ale można nim zarządzać [Rot 2008]. Ryzykowne sytuacje rodzą potrzebę szybkiego działania, eskalowania problemów, znajdowania rozwiązań. Potrzebne są zatem odpowiednie polityki i narzędzia w zakresie *Disaster Recovery Plan* i *Business Continuity Management*. Jak pisze M. Menon [Menon 2016], modne terminy, takie jak: *continuous availability*, *disaster avoidance*, *zero down-time*, *IT continuity*, w gruncie rzeczy oznaczają to samo. W dalszym ciągu mowa jest o DR, aczkolwiek z większym naciskiem na jego prewencyjne aspekty.

Biznes *always-on* stwarza presję na IT, żądając wyśrubowanych parametrów RTO (*Recovery Time Object* – wskaźnik pozwalający określić, jak długo będzie trwało odtwarzanie stanu bazy sprzed awarii systemu), RPO (*Recovery Point Objective* – wskaźnik określający, do jakiego punktu w czasie będziemy przywracać nasze dane) i umów SLA (*Service Level Agreement*). Jednocześnie plany usuwania skutków awarii pozostają jednym z największych wyzwań dla dyrektorów IT w podległym im obszarze zarządzania ciągłością działania. Choć wiele przedsiębiorstw dysponuje takimi planami, są one skomplikowane, często zawodne i trudne w realizacji, a także nieprzetestowane i przestarzałe. Utrudnia to zachowanie zgodności z regulacjami i utrzymanie stałej dostępności przedsiębiorstwa [Veeam Software 2016f]. Tematyka *Business Continuity Management* i będąca jej częścią *Disaster Recovery Planning* pozostają zatem cały czas bardzo istotne i aktualne.

Literatura

Białas A., 2006, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwa Naukowo-Techniczne, Warszawa.

BS 25999–1: 2006: *Business continuity management. Code of practice.*

BS 25999–2: 2007: *Specification for business continuity management*.

BSI Management Systems Polska Sp. z o.o.: *BS 25999 – Ciągłość biznesowa*, http://www.bsigroup.pl/pl/Auditowanie–i–certyfikacja/Systemy–zarzadzania/Normy–i–programy/BS–25999/ (15.09.2016).

DGA – *doradca bezpieczeństwa: Zarządzanie ciągłością działania (BS 25999)* http://security.dga.pl/page.php?13 (15.09.2016).

Gartner Analyst(s): Dave Russell, Pushan Rinnen, Robert Rhame, *Magic Quadrant for Data Center Backup and Recovery Software*, https://www.gartner.com/doc/reprints?id=1-38JSYOW&ct=160602&st=sb (15.09.2016).

Janas B., Perłowski W., 2007, *Od planów ciągłości działania do bezpieczeństwa informacji*, Akademia Wiedzy BCC, http://lepszybiznes.org/pad_files/aw_files/366_AW_SZBI_20070831.pdf (19.03.2016).

Kaczmarek T.T., Ćwiek G., 2009, *Ryzyko kryzysu a ciągłość działania*, Difin, Warszawa.

Menon M., 2016, *Is disaster recovery becoming obsolete? Continuity*, The Magazine of the Business Continuity Institute, http://www.thebci.org/index.php/is-disaster-recovery-becoming-obsolete, (21.10.2016).

Monkiewicz J., 2010, *Przedsiębiorstwo jako podmiot ryzyka: Rozwój koncepcji zarządzania ryzykiem*, [w:] Monkiewicz J., Gąsiorkiewicz L. (red.), *Zarządzanie ryzykiem działalności organizacji*, C.H. Beck, Warszawa.

Norma BS 25777, http://www.bcpguide.com/index.php?option=com_content&view=article&id=225%3Abs–25777&catid=64%3Acertyfikacja–normy–boks–1&Itemid=96 (12.09.2016).

Rot A., 2008, *IT risk assessment: Quantitative and qualitative approach*, [w:] Proceedings of the World Congress on Engineering and Computer Science (WCECS), IAENG, San Francisco, s. 1073-1078.

Rot A., 2016, *Zarzadzanie ryzykiem w cyberprzestrzeni – wybrane zagadnienia teorii i praktyki*, [w:] Komorowski T.M., Swacha J. (red.), *Projektowanie i realizacja systemów informatycznych zarządzania. Wybrane aspekty*, Polskie Towarzystwo Informatyczne PTI, Warszawa.

Staniec I., Zawiła-Niedźwiecki J., 2008, *Zarządzanie ryzykiem operacyjnym*, C.H. Beck, Warszawa.

Staniec I., Zawiła-Niedźwiecki J., 2015, *Ryzyko operacyjne w naukach o zarządzaniu*, C.H. Beck, Warszawa.

Veeam Software, 2016a, *Nowe rozwiązanie Veeam Availability Orchestrator umożliwia koordynację procesów usuwania skutków awarii*, https://www.veeam.com/pl/news/new-veeam-availability-orchestrator-enables-disaster-recovery-orchestration-for-the-always-on-enterprise.html#_ednref2 (19.10.2016).

Veeam Software, 2016b, *Veeam Availability Platform dla chmury hybrydowej*. https://www.veeam.com/pdf/ datasheet/veeam_availability_platform_hybrid_cloud_datasheet_pl.pdf, (27.10.2016).

Veeam Software, 2016c, *SureBackup – Weryfikacja poprawności kopii zapasowych*, https://www.veeam.com/pl/verified-recoverability.html?ad=features-submenu (29.10.2016).

Veeam Software, 2016d, *Veeam Backup & Replication*, https://www.veeam.com/pdf/datasheet/ veeam_backup_9_0_datasheet_pl.pdf (28.10.2016).

Veeam Software, 2016e, *Veeam ONE i Veeam ONE Free Edition*, https://www.veeam.com/pl/virtualization-management-one-solution.html (26.10.2016).

Veeam Software, 2016f, *Wykorzystanie potencjału danych*, https://www.veeam.com/pl/leveraged-data-virtual-lab.html?ad=features-submenu (26.10.2016).

Wołowski F., Zawiła-Niedźwiecki J., 2012, *Bezpieczeństwo systemów informacyjnych*, edu-Libri, Kraków-Warszawa.

Zapłata S., Kaźmierczak M., 2011, *Ryzyko, ciągłość biznesu, odpowiedzialność społeczna. Nowoczesne koncepcje zarządzania*, Oficyna Wolters Kluwer business, Warszawa.

Zawiła-Niedźwiecki J., 2007, *Metoda TSM–BCP projektowania rozwiązań zapewnienia ciągłości działania organizacji*, [w:] *Zarządzanie przedsiębiorstwem: Teoria i praktyka*, materiały konferencyjne, Akademia Górniczo-Hutnicza w Krakowie, Kraków, 22-23.11.2007.

Zawiła-Niedźwiecki J., Rostek K., Gąsiorkiewicz A. (red.), 2010, *Informatyka gospodarcza*, t. IV, C.H. Beck, Warszawa.

Zawiła-Niedźwiecki J., 2013, *Zarządzanie ryzykiem operacyjnym w zapewnieniu ciągłości działania organizacji*, edu-Libri, Kraków-Warszawa.