

INFORMACJA w (bez)ruchu

Działając we współczesnym otoczeniu biznesowym, organizacja musi sprostać wyzwaniom wielostronnej obsługi klientów. Uzależniona jest przy tym od dostępu do wielu technologii informatycznych, mogących usprawniać pracę i zwiększać wydajność. Bez względu na profil działalności żadna firma nie może w pełni wykorzystać swoich możliwości bez odpowiednich aplikacji biznesowych. Musi posiadać nowoczesne systemy informatyczne, pozwalające kontrolować procesy obsługi klienta, koordynować zbieranie informacji o rynku, a także umożliwiać przepływ informacji wewnątrz firmy.



Magdalena Bieganowska

Specjalista w Biurze Kontroli Wewnętrznej, zajmuje się weryfikacją i oceną procedur i procesów funkcjonujących w Spółkach Grupy, w tym oceną systemu kontroli wewnętrznej, absolwentka Wydziału Zarządzania Uniwersytetu Gdańskiego oraz studiów podyplomowych z zakresu audytu wewnętrznego, posiada międzynarodowe kwalifikacje audytora wewnętrznego CIA (Certified Internal Auditor), w Grupie Ergo Hestia od 2006 roku.



Magdalena Dłużewska

W Sopockim Towarzystwie Ubezpieczeń Ergo Hestia SA kieruje Działem ds. Bezpieczeństwa Informacji w Biurze Ryzyka i Bezpieczeństwa Informacji. Pełni funkcję Oficera Bezpieczeństwa Informacji oraz Zastępcy Koordynatora Zespołu Zarządzania Kryzysowego GEH. Ukończyła filologię polską na Uniwersytecie Gdańskim, absolwentka Bezpieczeństwa Europejskiego w Wyższej Szkole Ateneum. Jest pracownikiem Hestii od 1999 roku.

Każda instytucja finansowa powinna mieć System Zarządzania Bezpieczeństwem Informacji (SZBI). Obejmuje on politykę bezpieczeństwa informacji oraz plan zachowania ciągłości działania. Kompleksowo realizuje zatem zadania związane z minimalizacją prawdopodobieństwa wystąpienia incydentu/awarii oraz ograniczeniem niekorzystnego wpływu takich zdarzeń na funkcjonowanie organizacji i skróceniem czasu powracania do normalnej działalności firmy.

Jak chronić się przed... wyciekami informacji

Istotna jest świadomość, że bezpieczeństwo to dynamiczny, ciągle rozwijający się proces, a nie statyczny stan na „tu i teraz”. Zaprojektowanie i wdrożenie SZBI nie kończy się po jego ogłoszeniu. Konieczne są ciągły monitoring zmian zachodzących w organizacji (szczególnie zmian w środowisku IT), rozwój systemów wraz z rozwojem technologii informatycznych oraz cykliczne szkolenia pracowników.

Należy pamiętać ponadto, że ochrona informacji nie ogranicza się wyłącznie do danych przechowywanych i przesyłanych w systemach IT. Dotyczy również dokumentów papierowych przekazywanych z rąk do rąk i pozostawianych na biurkach oraz informacji przekazywanych ustnie, telefonicznie bądź za pomocą komunikatorów internetowych.

Każdy pracownik bez względu na zajmowane stanowisko codziennie przetwarza informacje będące własnością firmy. Dlatego wszyscy muszą być świadomi konieczności ochrony danych. Najwyższe kierownictwo powinno propagować politykę bezpieczeństwa i zwracać uwagę na potrzebę ochrony informacji, zaś każdy przełożony, sprawując bezpośredni nadzór nad pracownikiem, powinien go uświadamiać i pouczać, gdy zaistnieje taka konieczność.

Badania wykazują, że najczęstszą przyczyną niekontrolowanego wycieku informacji jest niestety niefrasobliwość pracowników. Transakcje są na ogół dość

Organizacja może inwestować w najlepsze systemy zabezpieczające, ale istotna jest również wiedza i wyobraźnia (często nieograniczona) pracowników.

dobrze zabezpieczone przez systemy, natomiast nie można tego samego powiedzieć o danych, którymi dysponują ludzie. Niebezpieczeństwo ze strony pracowników jest często dużo bardziej nieprzewidywalne niż zagrożenia z zewnątrz (na przykład ataki hakerów), ponieważ przed atakami informatycy mogą się zabezpieczyć, a przed bezmyślnym postępowaniem pracowników już niekoniecznie. To właśnie działanie ludzi - klientów i pracowników - powoduje zdarzenia zagrażające bezpieczeństwu informacji. Można tu wskazać przede wszystkim brak świadomości pracowników przetwarzających dane, często bowiem postępują oni zgodnie z najlepszą wolą, zamiast zgodnie z procedurami.

Organizacja może inwestować w najlepsze systemy zabezpieczające, ale istotna jest również wiedza i wyobraźnia (często nieograniczona) pracowników. Zachowując zdrowy rozsądek i znając procedury funkcjonujące w firmie, nie będą powodować swoim działaniem sytuacji zagrażających bezpieczeństwu.

Oczywiście poza nieumyślnymi przypadkami naruszeń bezpieczeństwa informacji możemy mieć również do czynienia ze świadomym działaniem pracownika na szkodę firmy lub klienta. Tego typu zachowanie jest już traktowane jak przestępstwo. Przykładem może być sytuacja w jednym z banków, którego pracownik dokonywał nieautoryzowanych transakcji na rachunkach klientów, wyprowadzając w ten sposób ponad 4 mln zł. Pracownikowi grozi kara pozbawienia wolności do 10 lat.

Kosz na śmieci...

Największym zagrożeniem w zakresie bezpieczeństwa informacji jest świadomość ludzi, a raczej jej brak. Systemy zabezpieczające mogą być zaprojektowane doskonale, ale efekty ich działania zależą od wiedzy użytkowników. Poza wyedukowaniem pracownika liczy się też odpowiednie przygotowanie jego miejsca pracy, na przykład sposób ustawienia kosza na śmieci. Obecnie większość dokumentów funkcjonuje w postaci elektronicznej, jednak pracownicy czasem je drukują, bo jest im tak łatwiej pracować, naniósł jakieś poprawki, które następnie wprowadzają w wersji elektronicznej. Dokument papierowy trafia do kosza (kosze najczęściej stoją obok biurka). Tymczasem zgodnie z Normą ISO 27001 kosze nie powinny znajdować się w zasięgu ręki pracownika - bezpośrednio przy jego stanowisku pracy. Powinny być postawione w kuchni i łazience, natomiast niepotrzebne dokumenty powinny znaleźć się w niszczarce. Przepis wydaje się drastyczny, jednak w przypadku niskiej świadomości pracowników co do charakteru dokumentów, którymi dysponują, może

być terapią wstrząsową, wymuszając na nich korzystanie z niszczarek. Konieczne jest tworzenie i propagowanie polityki bezpieczeństwa informacji. Trzeba szkolić ludzi, aby uświadomić im, że procedury nie mają utrudniać im życia, ale chronić interesy ich, klientów i firmy.

Utrata informacji

Ilość danych, jaką operują współczesne firmy, rośnie z roku na rok. Rozwijane są coraz to lepsze narzędzia, które przetwarzają te dane, a więc w coraz większym stopniu jesteśmy zależni od systemów informatycznych. Obecnie najczęściej spotykana przyczyną przestoju w działalności firm sektora finansowego są awarie systemów teleinformatycznych (w tym sieci telekomunikacyjnych), które czasami sporo kosztują...

Przyczyny niedostępności informacji

Dostępność oznacza, że uprawniony podmiot może korzystać z danych przez cały zdefiniowany na początku czas, w sposób wynikający z zakresu przyznanych uprawnień. Czas dostępności jest pochodną potrzeb biznesowych. Mówiąc o dostępności informacji, mamy na myśli przede wszystkim dostęp do aplikacji, oprogramowania systemowego i narzędziowego oraz dostępność sprzętu. System dostępny powinien być definiowany jako system działający wydajnie i stabilnie spełniający funkcjonalne wymagania użytkownika. Niedostępność informacji (z angielskiego *downtime*) możemy podzielić ze względu na trzy główne przyczyny:

- planowane wyłączenia
- nieplanowane wyłączenia
- katastrofy

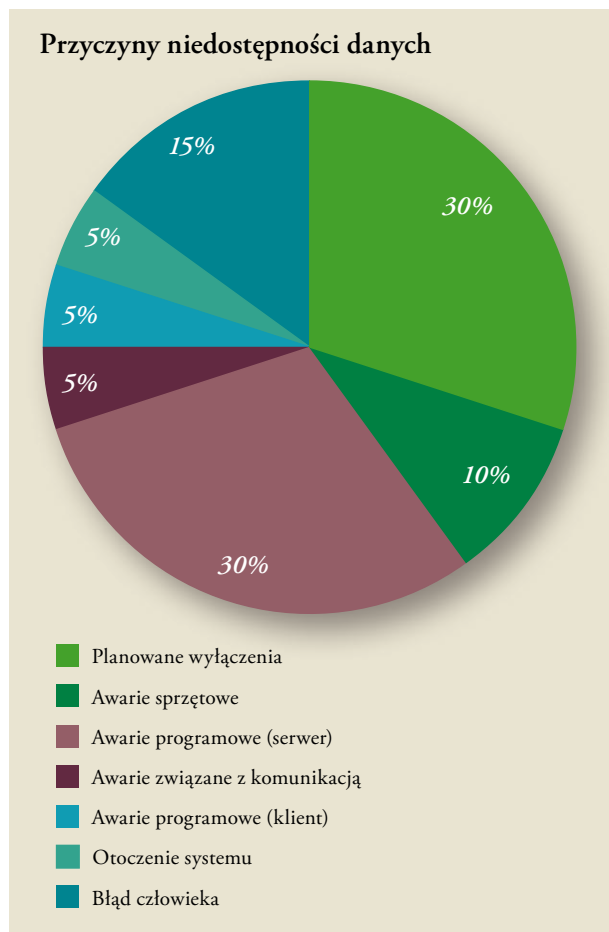
Planowane wyłączenia (z angielskiego *Planned outages*) najczęściej związane są wyłączeniem maszyn i urządzeń w celu przeprowadzenia różnych działań konserwacyjnych, koniecznością wymiany bądź rozbudowy sprzętu lub oprogramowania oraz z archiwizacją danych.

Nieplanowane wyłączenia (z angielskiego *Unplanned outages*) to m.in. przerwy w dostawie prądu, uszkodzenia sprzętu, awarie oprogramowania czy błędy człowieka.

Katastrofy (z angielskiego *Disaster*) najczęściej wynikają ze zdarzeń naturalnych, takich jak powodzie, pożary, trzęsienia ziemi lub powodowane są przez człowieka (np. atak terrorystyczny). Katastrofy odpowiadają za mniej niż 1% przypadków niedostępności danych.



Częstotliwość występowania różnych przyczyn niedostępności danych zależy od rodzajów systemów. Źródła pokazują różne wielkości. Poniższy rysunek przedstawia najczęściej podawane dane¹⁾.



Jak widać, awary sprzętowe stanowią jedynie około 10% przyczyn, podczas gdy najczęstszą przyczyną, odpowiedzialną za 40% awarii, są różnego rodzaju błędy programowe (łącznie awary: serwera, komunikacyjne i błędy klienta). Dość istotny udział w kategorii nieplanowanych wyłączeń mają również błędy ludzkie.

Drugą pod względem częstości przyczyną niedostępności systemów są planowane wyłączenia. Ta kategoria, odpowiednio zarządzana i monitorowana, nie powinna przynosić szkody użytkownikom i organizacji. Z podanej statystyki jasno wynika, że dobrze zaprojektowany system powinien umożliwiać wykonywanie wszelkich czynności administracyjnych w trakcie normalnego działania, bez przerw w udostępnianiu usług.

Wpływ braku dostępności danych na biznes

W literaturze przedmiotu można znaleźć pięć głównych kategorii skutków wpływu braku usług na działalność organizacji (mówimy tu o kluczowych systemie / systemach dla firmy).

Utrata produktywności (*Lost Productivity*)

Z powodu przerwy w działaniu systemu pracownicy nie mogą wykonywać swoich obowiązków. Utratę produktywności można wyliczyć w następujący sposób: strata = liczba godzin niedostępności systemu x (liczba pracowników x średnia stawka za godzinę pracy pracownika + średni przychód firmy na godzinę).

Utrata reputacji (*Damaged Reputation*)

Przerwa w działaniu systemu wpływa na jakość świadczonych usług przez firmę, a więc powoduje utratę zaufania u klientów, dostawców, partnerów biznesowych.

Utrata dochodu (*Lost Revenue*)

Przerwa w działaniu systemu może spowodować straty dla firmy (brak sprzedaży, odejście klientów z powodu niedotrzymania warunków umowy).

Wiarygodność finansowa (*Financial performance*)

Przerwa w działaniu systemu może spowodować utratę wartości akcji firmy na giełdzie, spadek wiarygodności kredytowej bądź nałożenie dodatkowych obostrzeń przez organy nadzoru.

Inne koszty (*Other expenses*)

Każda przerwa w działaniu systemu wiąże się z poniesieniem kosztów podniesienia systemów (koszty usług serwisu IT, koszty naprawy sprzętu bądź zakupu nowego).

Zarządzanie ciągłością i dostępnością systemów IT Jak utrzymać ciągłość działania?

Zarządzanie Ciągłością Usług IT zdefiniować można jako proces będący wsparciem dla procesu ciągłości biznesu, którego celem jest przywrócenie pracy systemu (bądź systemów) po wystąpieniu awarii w możliwie krótkim czasie.

W ostatnich czasach obserwujemy rosnącą zależność przedsiębiorstw od technologii, której celem jest wspieranie procesów biznesowych (m.in. produkcji, sprzedaży, czy obsługi klienta). Oczywiście dostępność systemów informatycznych i ciągłość ich pracy mają wpływ na funkcjonowanie firmy, dlatego czas, w jakim

przywracane są do pracy systemy po zaistniałej awarii, staje się parametrem krytycznym zarówno dla działów IT, jak i zarządzających procesami biznesowymi. Realizacja procesów biznesowych to zdolność do generowania zysków przez firmę. Sposób zabezpieczenia prowadzenia biznesu może być brany pod uwagę na przykład przez klienta, który chce podpisać z firmą duży kontrakt, lub przez firmę ubezpieczeniową przy wycenie ryzyka w ubezpieczeniu majątku firmy bądź odpowiedzialności cywilnej prowadzenia działalności gospodarczej, a nawet przez instytucje nadzorcze kontrolujące firmę.

Awarie (niedostępność informacji) są zdarzeniami losowymi (o przyczynach napisano wyżej), ale działania zmierzające do usunięcia tej awarii, która skutkuje częściowym lub całkowitym brakiem dostępu do systemu, powinny być odpowiednio zdefiniowane i zaplanowane. Mowa tu o przygotowaniu scenariuszy przywracania dostępności usług IT, wraz z określeniem maksymalnego czasu do tego potrzebnym.

W celu realizacji powyższych postulatów tworzy się Plan Odtwarzania po Katastrofie - *Disaster Recovery Plan* (DRP), który ma za zadanie zminimalizować ryzyko znacznego spowolnienia procesów realizowanych w firmie lub w skrajnych przypadkach całkowitego przerwania działalności firmy w wyniku braku dostępu do określonych zasobów informatycznych firmy. DRP jest traktowany jako część Planu Zachowania Ciągłości Działania - *Business Continuity Planning* (BCP) bądź jako odrębny dokument, który powinien być spójny z BCP.

Aby przygotować dobry DRP, należy przejść przez kilka odrębnych etapów.

I. Identyfikacja kluczowych procesów biznesowych w firmie.

II. Identyfikacja istotnych zasobów, do których możemy zaliczyć:

- zasoby ludzkie (administratorzy systemów, obsługa help-desk),
- systemy informatyczne,
- infrastruktura (serwery, łącza internetowe, sprzęt komputerowy).

Na tym etapie warto również określić niezbędne minimum dostępności zasobów, aby firma mogła funkcjonować.

III. Analiza zagrożeń, które mogą wystąpić oraz ustalenie strategii działania w przypadku ich wystąpienia.

Jeśli na tym etapie okaże się, że firma jest uzależniona od jakiegoś podmiotu zewnętrznego (dostawcy), należy dążyć do uzyskania od niego planów odtwarzania i zweryfikować, czy są one wystarczające.

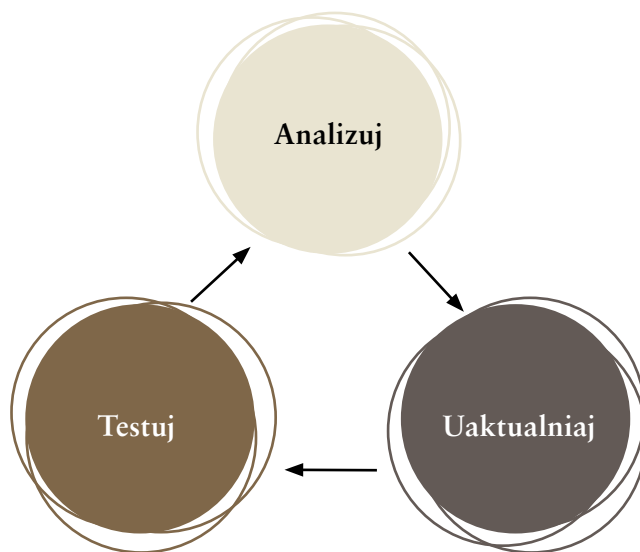
DRP jest to kompozycja środków organizacyjnych i technicznych umożliwiających utrzymanie ciągłości działania lub jak najszybsze odtworzenie najważniejszych procesów, przy minimalizacji wpływu zaistniałej sytuacji na działanie firmy. Finalna wersja **DRP** zawiera procedury odtworzenia dla wszystkich kluczowych zasobów informatycznych firmy. Każdy pracownik objęty okresowymi szkoleniami i testami, będzie posiadał wiedzę, która umożliwi mu szybkie wznowienie działania systemów w sytuacji kryzysowej.

Opracowanie Planu Odtwarzania po Katastrofie nie kończy się na jego przedstawieniu i zarchiwizowaniu. Daje on szansę organizacji na szybką reakcję i przywrócenie normalnej działalności w krótkim czasie, ale tylko pod warunkiem jego systematycznego testowania. Należy regularnie sprawdzać, jak przebiegają zaplanowane działania w odniesieniu do danego incydentu czy katastrofy. Niejednokrotnie bowiem dopiero w trakcie testów ujawniają się braki w opracowanych procedurach bądź okazuje się, że komunikacja między poszczególnymi zespołami kryzysowymi nie funkcjonuje w sposób prawidłowy.

Musimy również pamiętać o aktualizacji Planu. W każdej firmie wewnętrzne procesy są systematycznie optymalizowane i, co za tym idzie, pojawiają się nowe narzędzia i kolejne wersje systemów. A te zawsze niosą za sobą nierozpatrzone wcześniej ryzyka. Idealny **DRP** powinien żyć zgodnie z określonym schematem.

Działalność firmy jest potencjalnie narażona na niespodziewane zdarzenia, które mogą zaburzyć jej dotychczasowe działanie lub uniemożliwić normalne funkcjonowanie, co w praktyce może skutkować przerwą w działalności przedsiębiorstwa. 90% zdarzeń to tzw. „ciche katastrofy”, których się nie upublicznia, jednak ich wpływ na działalność przedsiębiorstwa jest znaczący. Mogą to być zarówno niekontrolowane wycieki wrażliwych informacji, które mają wpływ na biznes, jak i przerwy w dostępie do usług, czy innych zasobów firmy. Konsekwencje

Cykl życia DRP



zakłócenia ciągłości działania mogą być kosztowne: głównym ryzykiem jest utrata bieżących przychodów, a kolejne to kary finansowe czy koszty związane z pracą w nadgodzinach, co w dalszej perspektywie może skutkować koniecznością redukcji kosztów. Nie do oszacowania jest negatywny wpływ na wizerunek firmy czy utrata zaufania klientów i kontrahentów.

Podstawowym celem zarządzania ciągłością działania jest zapewnienie klientom dostępności usług lub produktów w sytuacji, gdy występują zakłócenia w normalnej działalności firmy. Wdrożenie Planu Odtwarzania po Katastrofie wraz z Planem Zachowania Ciągłości Działania jako elementu zarządzania firmą daje korzyści nie tylko w chwili wystąpienia awarii, ale też zwiększa wiarygodność przedsiębiorstwa. Gotowość do działania w przypadku wystąpienia katastrofy, czy innych zdarzeń zakłócających normalne funkcjonowanie organizacji, poprzez utrzymanie funkcjonowania najistotniejszych obszarów biznesowych na minimalnym akceptowalnym poziomie, decyduje często o dalszym „być albo nie być” firmy.

Decyzja o zbudowaniu planu ma charakter strategiczny i jest wyrazem rzeczywistej troski zarządu przedsiębiorstwa o jego przyszłość. Posiadanie planu podnosi wiarygodność firmy w oczach udziałowców, inwestorów i klientów, a coraz częściej jest również wymogiem stawianym przez regulatorów i ubezpieczycieli.

Magdalena Bieganowska
magdalena.bieganowska@ergohestia.pl
Magdalena Dłużewska
magdalena.dluzewska@ergohestia.pl

¹⁾ Evan Marcus, Hal Stern, *Blueprints for High Availability- Designing Resilient Distributed Systems*