PROBLEM? WYLUZUJ. OGARNIESZ TO!

Internet Zniknął na Tydzień i Moja Firma Razem z Nim

Jak rozpoznawać zależności firmy od sieci i usług chmurowych, przygotować tryb pracy zastępczej oraz ustalić komunikację z klientami bez improwizowania planu ciągłości po awarii



Max Paradox

Internet Zniknął na Tydzień i Moja Firma Razem z Nim

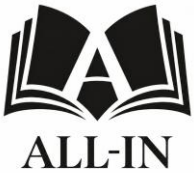
Jak rozpoznawać zależności firmy od sieci i usług chmurowych, przygotować tryb pracy zastępczej oraz ustalić komunikację z klientami bez improwizowania planu ciągłości po awarii

Max Paradox

PROBLEM? WYLUZUJ. OGARNIESZ TO!

ISBN: 9788384839119

ALL-IN Rafał Płonkowski



SPIS TREŚCI

INTRO 5

Rozdział 1 - Firma na niewidzialnym kablu 10

Rozdział 2 - Kto naprawdę trzyma klucze do Twoich procesów? 19

Rozdział 3 - Zapasowy internet nie uratuje firmy, jeśli problem leży gdzie indziej 28

Rozdział 4 - Gdy każdy ratuje firmę po swojemu 36

Rozdział 5 - Tryb awaryjny, którego nikt nie potrafi uruchomić 45

Rozdział 6 - Dane są bezpieczne. Tylko gdzie właściwie są? 53

Rozdział 7 - Kiedy komunikator milczy, plotka przejmuje dowodzenie 62

Rozdział 8 - Dostawca obiecał pomoc. Firma nadal stoi 70

Rozdział 9 - Co ratować najpierw, kiedy wszystkiego uratować się nie da? 79

Rozdział 10 - Ręcznie nie znaczy na chybił trafił: proces zastępczy od początku do końca 88

Rozdział 11 - Klient nie potrzebuje technicznej diagnozy. Potrzebuje odpowiedzi 98

Rozdział 12 - Siedem dni bez sieci: jak zarządzać firmą, kiedy awaria nie chce się skończyć 107

Rozdział 13 - Plan ciągłości działania, który nie potrzebuje własnego instruktażu 116

Rozdział 14 - Próba generalna katastrofy, podczas której niczego nie trzeba niszczyć 124

Rozdział 15 - To nie musi być zwykła awaria. Kiedy ratowanie firmy może pogorszyć sytuację 133
Rozdział 16 - Plan się posypał, a awaria przyszła z koleżanką 140
Rozdział 17 - Gdy chmura nie wraca, a firmę trzeba z niej wyprowadzić 149
Rozdział 18 - Plan działał w zeszłym roku. Szkoda, że firma jest już inna 158
Rozdział 19 - Internet wrócił. Teraz policz, co naprawdę się wydarzyło 166
Rozdział 20 - Firma, która nie czeka na cud: od pomysłu do prawdziwej gotowości 174

INTRO

Jest poniedziałek, godzina 9:07. Kawa jeszcze ciepła, zespół właśnie zaczyna pracę, a Ty masz całkiem przyzwoity plan na nadchodzący tydzień. Wchodzisz do systemu, żeby sprawdzić zamówienia. Strona się nie ładuje. Odświeżasz. Nic. Próbujesz otworzyć pocztę. Błąd połączenia. Komunikator również milczy, choć zwykle o tej porze ktoś zdążył już wysłać siedem wiadomości z pytaniem, czy widziałeś poprzednie sześć. Ktoś z drugiego końca biura rzuca: „U was też nie działa?". Oczywiście. Właśnie rozpoczęło się zebranie, na które nikt nie wysłał zaproszenia, a którego jedynym punktem programu jest zbiorowe wpatrywanie się w obracające kółeczko ładowania.

Przez pierwsze dziesięć minut sytuacja wygląda niewinnie. Router pewnie potrzebuje restartu. Dostawca internetu zapewne coś naprawia. Administrator sprawdzi, ktoś zadzwoni, zaraz wrócimy do pracy. Po godzinie atmosfera jest już mniej towarzyska. Nie można wystawić faktur, sprawdzić historii klientów ani potwierdzić części zamówień. Dokumenty są bezpiecznie przechowywane w chmurze, co okazuje się wyjątkowo pocieszające, zważywszy na fakt, że nikt nie może ich otworzyć. Po trzech godzinach odkrywasz, że numer telefonu do firmy obsługującej najważniejszy system znajduje się w skrzynce mailowej. Tej samej, która nie działa. Gratulacje. Twoja procedura ratunkowa właśnie zamknęła się we własnej szafie i wyrzuciła klucz.

A teraz wyobraź sobie, że awaria nie kończy się po lunchu. Nie kończy się również następnego ranka. Trwa tydzień. Siedem dni, podczas których firma nadal ma klientów, zobowiązania, pracowników, koszty i terminy, ale straciła dostęp do części narzędzi, które pozwalały jej funkcjonować. Możesz mieć najlepszy produkt na rynku, kompetentny zespół i świetnie zaprojektowaną

stronę internetową. Jeżeli podstawowe czynności wymagają jednoczesnego działania kilku zewnętrznych usług, wszystkie te zalety mogą nagle zostać sprowadzone do jednego zdania: „Przepraszamy, aktualnie mamy problemy techniczne".

Najbardziej zdradliwe jest to, że przed awarią wszystko mogło działać znakomicie. Nowoczesne firmy przenoszą do internetu sprzedaż, księgowość, obsługę klientów, dokumentację, komunikację i zarządzanie projektami. Każde takie usprawnienie ma sens. Automatyzacja ogranicza ręczną pracę, wspólne pliki przyspieszają współpracę, a aplikacje chmurowe pozwalają prowadzić firmę praktycznie z dowolnego miejsca. Kłopot zaczyna się wtedy, gdy wygoda zostaje pomylona z niezawodnością. Dostępność systemu przez ostatnie dwa lata nie jest dowodem, że będzie dostępny dokładnie w chwili, kiedy najbardziej go potrzebujesz. To trochę tak, jakby uznać, że skoro od dawna nie zgubiłeś kluczy, drzwi wejściowe przestały ich wymagać.

Co więcej, awaria internetu nie zawsze oznacza awarię samego łącza. Połączenie może działać, ale niedostępna będzie usługa chmurowa, przez którą przechodzą zamówienia. System może funkcjonować, lecz logowanie zostanie zablokowane przez niedziałającą usługę uwierzytelniania. Pracownik może mieć kopię potrzebnego dokumentu, ale bez dostępu do aktualnych danych nie będzie wiedział, czy przypadkiem nie pracuje na wersji sprzed trzech tygodni. Z perspektywy klienta te różnice są często mało istotne. On nie zamawiał analizy infrastruktury informatycznej. Zamawiał usługę, produkt albo odpowiedź i chciałby wiedzieć, co dalej.

Właśnie dlatego przygotowanie firmy na dłuższą niedostępność sieci zaczyna się od znacznie ciekawszego pytania niż „Czy mamy zapasowy internet?". Trzeba ustalić, co rzeczywiście musi się wydarzyć, aby firma mogła wykonywać swoją pracę, oraz które elementy tego procesu zależą od usług pozostających poza jej kontrolą. Czasami zapasowe połączenie komórkowe rozwiąże

większość problemów. Innym razem pomoże mniej więcej tyle, co drugi pilot do telewizora podczas awarii zasilania. Jeżeli nie działa centralny system dostawcy, dodatkowe łącze nie przywróci jego działania. Bez znajomości tych zależności można wydać sporo pieniędzy na zabezpieczenia, które świetnie wyglądają w prezentacji, ale nie ratują najważniejszych operacji.

Nie musisz przy tym zmieniać firmy w bunkier technologiczny, drukować całej bazy klientów ani zatrudniać człowieka, którego jedynym obowiązkiem będzie strzeżenie segregatora z napisem „KONIEC INTERNETU". Odporność organizacji nie polega na utrzymywaniu drugiej, identycznej firmy na wypadek awarii pierwszej. Chodzi o świadome wybranie działań, które naprawdę muszą być kontynuowane, określenie dopuszczalnych opóźnień i przygotowanie prostszego sposobu pracy tam, gdzie jest on możliwy. Niektóre zadania mogą poczekać. Inne wymagają natychmiastowej reakcji. Jeszcze inne trzeba bezpiecznie zatrzymać, ponieważ wykonywanie ich bez aktualnych informacji mogłoby narobić więcej szkód niż sama przerwa.

Szczególnie ważne jest rozróżnienie pomiędzy posiadaniem danych a możliwością sensownego wykorzystania ich podczas awarii. Kopia zapasowa przechowywana w tej samej niedostępnej usłudze nie zapewnia pracy offline. Wydrukowana lista kontrahentów może się przydać, ale niesie również obowiązek odpowiedniego zabezpieczenia informacji. Awaryjny arkusz z zamówieniami pomoże tylko wtedy, gdy wiadomo, kto go prowadzi, jakie dane wolno do niego wpisywać i jak później przenieść informacje do głównego systemu bez zdublowania transakcji. Improwizacja bywa twórcza podczas firmowej integracji. Przy rozliczeniach finansowych i danych klientów jej walory artystyczne są zdecydowanie mniej pożądane.

Drugą stroną problemu są ludzie. Pracownicy potrzebują wiedzieć, kto podejmuje decyzje, gdzie zgłaszać problemy i które zadania mają pierwszeństwo. Klienci oczekują informacji, nawet

jeżeli odpowiedź brzmi: „Nie znamy jeszcze terminu przywrócenia pełnej obsługi”. Cisza zwykle nie poprawia sytuacji. Pozostawia przestrzeń dla domysłów, ponawianych telefonów i narastającej frustracji. Jednocześnie komunikat wysłany w pośpiechu, zawierający niepotwierdzoną obietnicę usunięcia awarii za trzydzieści minut, potrafi zamienić jeden problem w dwa. Dlatego warto wcześniej ustalić kanały kontaktu, odpowiedzialność za komunikaty i sposób aktualizowania informacji, również wtedy, gdy standardowa poczta i komunikator pozostają niedostępne.

Ta książka pomoże Ci spojrzeć na firmę nie jak na zbiór aplikacji, lecz jak na sieć rzeczywistych działań, decyzji i zależności. Nauczysz się rozpoznawać procesy najbardziej wrażliwe na przerwy w dostępie, odróżniać potrzebne zabezpieczenia od kosztownych pozorów bezpieczeństwa oraz przygotowywać zastępcze sposoby pracy z uwzględnieniem ich ograniczeń. Zobaczysz również, dlaczego plan ciągłości działania powinien być zrozumiały dla osób, które będą go wykonywały, a nie wyłącznie dla tych, które potrafią narysować imponujący diagram. Procedura, której nikt nie rozumie pod presją, jest przede wszystkim dokumentem. Często bardzo eleganckim dokumentem.

Nie znajdziesz tutaj obietnicy, że odpowiedni zestaw narzędzi uchroni Cię przed każdą awarią. Niektóre zdarzenia wymagają pomocy specjalistów, szczególnie gdy istnieje podejrzenie cyberataku, naruszenia danych lub zagrożenia bezpieczeństwa. Nie każdą usługę da się zastąpić ręczną procedurą i nie każda firma może sobie pozwolić na identyczny poziom przygotowania. Można jednak ograniczyć chaos, przewidzieć najważniejsze decyzje i sprawić, że nawet poważna przerwa nie musi oznaczać całkowitej utraty kontroli.

Najlepiej rozpocząć przygotowania wtedy, gdy systemy jeszcze działają, klienci są spokojni, a administrator nie odbiera jednocześnie czterech telefonów. Wystarczy uczciwie przyjrzeć się własnej organizacji i zapytać: co zrobilibyśmy jutro rano, gdyby

nasze najważniejsze usługi internetowe przestały odpowiadać? Jeżeli pierwszą odpowiedzią jest „Poczekalibyśmy, aż wrócą”, masz już bardzo dobry powód, żeby czytać dalej.

Internet kiedyś wróci. Znacznie ważniejsze jest to, czy Twoja firma będzie potrafiła sensownie funkcjonować, zanim to nastąpi.

Rozdział 1 - Firma na niewidzialnym kablu

Właściciel niewielkiej hurtowni przez lata powtarzał, że jego firma jest odporna na techniczne niespodzianki. Miał dwa komputery zapasowe, porządny serwer plików i człowieka od informatyki, który odbierał telefon nawet wtedy, gdy normalni ludzie oglądali już serial. Pewnego czwartku o 14:20 pracownik magazynu próbował wydrukować etykietę na przesyłkę. System odmówił współpracy. Kilka minut później okazało się, że zamówienia są widoczne, ale nie można przekazać ich do firmy kurierskiej. Po kolejnych dwudziestu minutach ktoś odkrył, że rozwiązanie problemu wymaga zalogowania się do panelu dostawcy, a logowanie korzysta z zewnętrznej usługi, która właśnie miała awarię. Trzydzieści osób, trzydzieści stanowisk pracy i jeden niewidzialny element infrastruktury, którego nazwy większość zespołu nigdy wcześniej nie słyszała. Gdyby ogłoszono konkurs na najdroższą rzecz, której nikt nie zauważa, znalazłaby się wysoko w rankingu.

Ta przykładowa historia pokazuje podstawowy problem współczesnej firmy. Jej działalność coraz rzadziej zależy wyłącznie od sprzętu stojącego w biurze i ludzi zatrudnionych na miejscu. Nawet niewielka organizacja korzysta z wielu usług, połączeń, kont i integracji, które działają gdzieś poza jej bezpośrednią kontrolą. Codziennie wymieniają między sobą informacje, potwierdzają uprawnienia, aktualizują stany magazynowe i przesyłają dokumenty. Dopóki funkcjonują prawidłowo, pozostają praktycznie niewidoczne. Pracownik klika przycisk, system wykonuje polecenie, klient otrzymuje potwierdzenie. Nikt nie zastanawia się, ile niezależnych elementów musiało współpracować, aby ten przycisk rzeczywiście coś zrobił. Odkrywanie całego mechanizmu zwykle zaczyna się dopiero wtedy, gdy przycisk przestaje działać. To dość osobliwy sposób poznawania własnego przedsiębiorstwa,

zwłaszcza że lekcja często odbywa się w godzinach pracy i jest wyjątkowo droga.

Pierwszym krokiem do przygotowania firmy na awarię jest zrozumienie różnicy pomiędzy korzystaniem z technologii a zależnością od technologii. Korzystasz z narzędzia wtedy, gdy ułatwia Ci wykonanie zadania. Jesteś od niego zależny wtedy, gdy bez niego zadanie staje się niemożliwe, niebezpieczne albo tak powolne, że traci ekonomiczny sens. Arkusz kalkulacyjny może pomagać w analizowaniu sprzedaży, ale jeśli wszystkie kluczowe dane znajdują się wyłącznie w internetowym systemie raportowym, sam arkusz niewiele uratuje. Telefon służbowy ułatwia kontakt z klientami, lecz jeżeli numer klienta jest dostępny tylko po zalogowaniu do CRM, nawet najdroższy smartfon staje się eleganckim przedmiotem służącym do oglądania własnej frustracji. Zależność nie wynika więc z obecności aplikacji. Wynika z tego, że bez konkretnej aplikacji, połączenia lub informacji nie można wykonać ważnej czynności.

To rozróżnienie ma praktyczne znaczenie, ponieważ firmy często analizują swoje bezpieczeństwo technologiczne, patrząc przede wszystkim na urządzenia. Ile mamy komputerów? Czy router jest nowoczesny? Czy wykupiliśmy dodatkową ochronę? Czy dostawca chmury jest renomowany? Wszystkie te pytania bywają uzasadnione, ale nie mówią jeszcze, co stanie się z działalnością, kiedy jeden element przestanie odpowiadać. Właściciel może mieć doskonale zabezpieczone laptopy i jednocześnie nie wiedzieć, że wszystkie zamówienia przechodzą przez pojedynczą integrację, której awaria zatrzyma sprzedaż. Może też mieć dwa niezależne łącza internetowe, lecz korzystać z jednej usługi logowania do wszystkich najważniejszych systemów. Z punktu widzenia użytkownika wygląda to na rozbudowaną infrastrukturę. Z punktu widzenia awarii jest to jedna brama z bardzo dużą liczbą ozdobnych klamek.

Nie wszystkie awarie są sobie równe

Warto przyjrzeć się temu, co właściwie oznacza zdanie „Nie działa nam internet”. Dla jednego przedsiębiorstwa będzie to brak dostępu do stron internetowych i poczty. Dla drugiego problem z połączeniem sieciowym między oddziałami. Dla trzeciego niedostępność aplikacji chmurowej, mimo że przeglądarka bez problemu otwiera inne strony. Może również dojść do uszkodzenia sprzętu, błędnej konfiguracji sieci, przerwy u operatora, awarii zewnętrznego centrum danych lub problemu z usługą potwierdzającą tożsamość użytkownika. Objawy mogą wyglądać podobnie, ale przyczyny i możliwe działania różnią się zasadniczo. Restartowanie routera podczas awarii usługi chmurowej jest mniej więcej tak skuteczne jak wielokrotne naciskanie przycisku windy, kiedy budynek nie ma zasilania. Daje poczucie zaangażowania, lecz rzadko przyspiesza naprawę.

Jeszcze trudniejsze są sytuacje, w których część systemów działa prawidłowo. Sprzedawca widzi zamówienie, ale magazyn nie otrzymuje informacji o jego realizacji. Księgowość może wystawić dokument, lecz nie jest w stanie potwierdzić, czy płatność została zaksięgowana. Dział obsługi klientów przyjmuje zgłoszenia, ale nie ma dostępu do historii wcześniejszych kontaktów. Takie awarie nie zatrzymują firmy w sposób oczywisty. Zamiast tego powodują powstawanie błędów, opóźnień i rozbieżności, które mogą ujawnić się dopiero po przywróceniu systemów. Pracownicy nadal wykonują zadania, więc kierownictwo ma wrażenie, że sytuacja pozostaje pod kontrolą. Tymczasem organizacja produkuje zaległości szybciej, niż będzie potrafiła je później uporządkować. Szczególnie niebezpieczne jest ręczne wykonywanie operacji bez wiedzy, czy system automatyczny również ich nie zrealizował.

Dlatego warto oddzielić trzy sprawy: awarię techniczną, jej wpływ na proces oraz konsekwencję biznesową. Niedostępność platformy sprzedażowej jest zdarzeniem technicznym. Brak możliwości przyjmowania zamówień oznacza zakłócenie procesu. Utrata sprzedaży, opóźnienie dostawy lub niezadowolenie klienta

stanowią konsekwencję biznesową. Te poziomy często miesza się w jednej rozmowie, co utrudnia podejmowanie decyzji. Administrator wyjaśnia, że usługa nie odpowiada na zapytania, handlowiec mówi, że nie może obsługiwać klientów, a dyrektor pyta, ile pieniędzy właśnie tracimy. Każdy opisuje ten sam problem, ale z innej strony. Aby zdecydować, co robić, trzeba połączyć te informacje. Nie wystarczy wiedzieć, co się zepsuło. Trzeba rozumieć, co z tego wynika dla działalności przedsiębiorstwa.

Najprostszym sposobem oceny znaczenia problemu jest sprawdzenie, jak zmieniają się jego skutki wraz z czasem. Awaria trwająca piętnaście minut może być niewygodna, ale niegroźna. Po czterech godzinach może już spowodować opóźnienia w wysyłkach. Następnego dnia przedsiębiorstwo zacznie odczuwać utratę przychodów lub problemy z realizacją zobowiązań. Po tygodniu konsekwencje mogą dotyczyć płynności finansowej, reputacji i relacji z najważniejszymi kontrahentami. Nie ma jednak jednej uniwersalnej granicy. Firma projektowa może bez większych strat przesunąć wewnętrzne spotkanie o dwa dni, podczas gdy przedsiębiorstwo obsługujące pilne zgłoszenia serwisowe musi reagować niemal natychmiast. O znaczeniu procesu nie decyduje liczba osób, które go wykonują, lecz konsekwencje jego zatrzymania.

W praktyce dobrym początkiem jest krótkie ćwiczenie. Wybierz pięć czynności, które Twoja firma wykonuje niemal każdego dnia, i przy każdej zadaj sobie trzy pytania. Co stanie się, jeżeli nie wykonamy jej przez cztery godziny? Jakie konsekwencje pojawią się po jednym dniu? Co wydarzy się po tygodniu? Nie próbuj od razu wyceniać każdej minuty przestoju z dokładnością właściwą rozliczeniom podatkowym. Wystarczy ustalić, czy pojawi się niewygoda, realna strata, naruszenie zobowiązań albo zagrożenie dla bezpieczeństwa. Jeżeli odpowiedź brzmi „trudno powiedzieć”, nie wpisuj automatycznie „brak ryzyka”. Zapisz, czego nie wiesz i

kto może pomóc to ustalić. Brak wiedzy jest problemem, ale zdecydowanie tańszym, kiedy zostanie odkryty przed awarią.

Wygoda ma swoich ukrytych wspólników

Jednym z największych źródeł ryzyka jest przekonanie, że skoro firma korzysta z kilku różnych dostawców, jej systemy są od siebie niezależne. W rzeczywistości wiele aplikacji może korzystać z tej samej usługi uwierzytelniania, dostawcy infrastruktury chmurowej, operatora sieciowego lub mechanizmu wymiany danych. Awaria jednego elementu potrafi więc wpłynąć na pozornie niezwiązane obszary. Pracownicy zauważają, że jednocześnie nie działa księgowość, komunikator i system sprzedażowy. Naturalnym podejrzeniem staje się rozległy problem z internetem, chociaż wspólną przyczyną może być wyłącznie niedostępność usługi odpowiedzialnej za logowanie. Oddzielne logo na ekranie nie oznacza oddzielnego ryzyka. Gdyby tak było, wystarczyłoby zmienić tapetę w komputerze, aby uzyskać niezależną infrastrukturę.

Szczególnie zdradliwe są zależności związane z dostępem. Można posiadać sprawną aplikację, aktualne dane i działające połączenie, a mimo to nie móc rozpocząć pracy. Powodem bywa niedostępne konto administratora, wygaśnięta sesja użytkownika albo brak możliwości potwierdzenia logowania. Wyobraź sobie, że jedyna osoba mająca uprawnienia do zmiany konfiguracji wyjechała na urlop. Jej telefon służbowy służy jednocześnie do odbierania kodów autoryzacyjnych. Firma posiada więc dostęp administracyjny, ale praktycznie nie może go wykorzystać. Problem nie polega na tym, że zabezpieczenia są niepotrzebne. Przeciwnie, powinny chronić przed nieuprawnionym dostępem również podczas awarii. Chodzi o to, aby bezpieczne odzyskanie dostępu nie zależało od obecności jednej osoby i jednego urządzenia.

Inną niewidzialną zależnością są dane. System może być dostępny, ale informacje niezbędne do podjęcia decyzji mogą

znajdować się gdzie indziej. Handlowiec zna cenę produktu, lecz nie wie, czy magazyn potwierdził jego dostępność. Osoba odpowiedzialna za realizację usług posiada harmonogram, ale nie ma aktualnej listy zmian uzgodnionych z klientami. Zarząd otrzymuje raport sprzedaży, który wygląda wiarygodnie, choć część transakcji nie została jeszcze zsynchronizowana. W każdym takim przypadku zagrożeniem jest nie tylko brak informacji, ale także nadmierna pewność, że informacje widoczne na ekranie są kompletne. Praca na starych danych może prowadzić do większych strat niż czasowe wstrzymanie czynności. Czasami najbardziej profesjonalną decyzją jest powiedzenie: „Nie potwierdzimy tego, dopóki nie sprawdzimy aktualnego stanu".

Wiele organizacji reaguje na ryzyko odruchem kupowania kolejnych zabezpieczeń. Dodatkowy serwer, następny abonament, drugi operator, osobna aplikacja do komunikacji. Każde rozwiązanie może być użyteczne, pod warunkiem że odpowiada na konkretny problem. Jeżeli firma nie wie, które czynności wymagają ciągłego dostępu do danych, łatwo zabezpieczy to, co najlepiej rozumie jej dział IT, zamiast tego, co najbardziej boli klientów. Można wydać znaczną kwotę na utrzymanie wewnętrznego systemu raportowego, a jednocześnie pozostawić bez zabezpieczenia pojedynczy kanał przyjmowania zamówień. Technologia nie staje się wartościowa dlatego, że kosztuje dużo albo jej nazwa wygląda dobrze na fakturze. Jej wartość w sytuacji awaryjnej wynika z tego, jaką rzeczywistą stratę pomaga ograniczyć.

Ważna jest również zależność od dostawców, których firma nigdy nie postrzegała jako elementu własnej infrastruktury. Przykładowo przedsiębiorstwo może korzystać z platformy do obsługi płatności, a ta z kolejnych usług przetwarzających transakcje. Integracja ze sklepem może wymagać prawidłowego działania zewnętrznego interfejsu. Wysłanie powiadomienia do klienta może zależeć od dostawcy poczty lub wiadomości SMS. Nie

musisz znać każdego technicznego podwykonawcy, aby prowadzić działalność. Warto jednak wiedzieć, które usługi są krytyczne, jak zgłaszać ich awarie i czy dostawca udostępnia informacje o stanie działania. Nie zakładaj też, że każda przerwa oznacza niewywiązanie się z umowy. Rzeczywiste obowiązki, gwarancje i zasady rekompensat wynikają z konkretnych warunków świadczenia usług.

Najdroższe zdanie w firmie

„Jakoś sobie poradzimy" jest jednym z najbardziej popularnych nieformalnych planów ciągłości działania. Brzmi rozsądnie, odważnie i nie wymaga przygotowania dokumentacji. Ma jednak poważną wadę: każdy pracownik rozumie je inaczej. Dla jednego oznacza zapisywanie zamówień na kartkach. Dla drugiego wysyłanie informacji z prywatnej poczty. Dla trzeciego samodzielne podejmowanie decyzji o rabatach, zwrotach i terminach dostawy. W normalnych warunkach takie działania byłyby prawdopodobnie przedmiotem dyskusji z przełożonym. Podczas awarii mogą zostać uznane za godną pochwały inicjatywę. Dopiero po przywróceniu systemów okazuje się, że firma ma trzy wersje prawdy, dwie listy zamówień i jednego klienta, któremu obiecano dostawę produktu sprzedanego już komuś innemu.

Nie oznacza to, że pracownikom należy zakazać samodzielności. Przeciwnie, dobrze przygotowana organizacja potrafi działać dzięki ich inicjatywie. Potrzebuje jednak ustalonych granic, w których można podejmować decyzje bez pytania o każdą drobnostkę. Kto może przyjąć zamówienie ręcznie? Jakie informacje należy zanotować? Które operacje wymagają późniejszego potwierdzenia? Kiedy trzeba przerwać działanie ze względu na ryzyko błędu? Odpowiedzi powinny wynikać z rzeczywistych potrzeb firmy, a nie z uniwersalnego dokumentu pobranego z internetu. Dobrze opisany sposób pracy zastępczej nie jest instrukcją zachowania spokoju. Jest sposobem ograniczenia liczby decyzji, które ludzie będą musieli podejmować w najgorszym możliwym momencie.

Zanim jednak firma przygotuje takie zasady, powinna uczciwie rozpoznać swoją sytuację. Pomaga w tym obserwacja zwyczajnego dnia pracy. Zamiast pytać każdego pracownika, z jakich aplikacji korzysta, poproś go o opisanie rzeczywistych czynności. Co otrzymuje na początku zadania? Jakie informacje sprawdza? Co przekazuje dalej? Skąd wie, że praca została wykonana poprawnie? W którym momencie potrzebuje połączenia z siecią lub zewnętrznej usługi? Odpowiedzi bywają zaskakujące. Często okazuje się, że najważniejsza zależność nie dotyczy rozbudowanego systemu, ale drobnego etapu, bez którego nie można zakończyć całej operacji. Na przykład potwierdzenia numeru zlecenia, pobrania aktualnej ceny albo uzyskania zgody osoby pracującej w innym oddziale.

Takie obserwacje pomagają też oddzielić rzeczywiste potrzeby od przyzwyczajeń. Niektóre czynności wykonujemy online dlatego, że jest to najwygodniejsza metoda, a nie dlatego, że wymaga tego charakter pracy. Inne rzeczywiście muszą korzystać z aktualnych danych i bezpiecznego połączenia. Rozpoznanie tej różnicy otwiera drogę do rozsądnych decyzji. Firma nie powinna próbować utrzymywać wszystkich funkcji za wszelką cenę, jeżeli wystarczy zapewnić ciągłość najważniejszych działań. Nie powinna również uruchamiać ręcznych obejść tam, gdzie mogłyby one naruszać bezpieczeństwo danych, prowadzić do błędnych rozliczeń lub tworzyć zobowiązania niemożliwe do spełnienia. Profesjonalizm nie zawsze polega na nieprzerwanym działaniu. Czasem polega na rozpoznaniu chwili, w której należy bezpiecznie zatrzymać proces.

Na koniec spójrz na własną firmę z perspektywy klienta, który nie ma pojęcia, jakich aplikacji używasz. Nie interesuje go, czy zawiodło łącze, dostawca infrastruktury czy system autoryzacji. Chce wiedzieć, czy jego zamówienie zostało przyjęte, czy usługa będzie wykonana i kiedy otrzyma wiarygodną informację. To właśnie te oczekiwania powinny wyznaczać kierunek przygotowań. Jeżeli potrafisz wskazać, jakie obietnice składasz klientom i które

zależności mogą uniemożliwić ich dotrzymanie, zaczynasz rozumieć własne ryzyko znacznie lepiej niż przedsiębiorca posiadający wyłącznie imponującą listę wykupionych systemów.

Nie musisz znać każdego przewodu, serwera i protokołu komunikacyjnego. Musisz natomiast wiedzieć, które niewidzialne elementy podtrzymują najważniejsze działania Twojej organizacji. Firma może funkcjonować dzięki technologii, ale powinna być zarządzana przez ludzi, którzy rozumieją konsekwencje jej niedostępności. Inaczej nie jest przedsiębiorstwem korzystającym z internetu. Jest przedsiębiorstwem liczącym na to, że internet nigdy nie zrobi sobie wolnego.

Rozdział 2 - Kto naprawdę trzyma klucze do Twoich procesów?

Wyobraź sobie, że zapraszasz kierowników działów na spotkanie i prosisz o wskazanie systemów niezbędnych do działania firmy. Przedstawiciel sprzedaży wymienia CRM. Księgowość wskazuje program finansowy. Magazyn potrzebuje systemu stanów magazynowych, a dział administracji zapewnia, że bez poczty elektronicznej wszyscy możemy właściwie wracać do domu. Po czterdziestu minutach tablica jest pełna nazw aplikacji, strzałek i skrótów. Wygląda imponująco. Niestety nadal nie wiadomo, czy jutro będzie można obsłużyć klienta, jeżeli jedna z tych usług przestanie działać. Powstał bowiem katalog narzędzi, a nie mapa zależności. To trochę tak, jakby próbować wyjaśnić działanie restauracji, sporządzając spis wszystkich garnków. Informacja niewątpliwie interesująca, ale klient zamawiający obiad oczekuje czegoś więcej niż zapewnienia, że kuchnia posiada dwanaście rondli.

Prawdziwa mapa zależności zaczyna się od tego, co przedsiębiorstwo robi, a dopiero później przechodzi do technologii. Jej zadaniem jest pokazanie, jak konkretne działanie prowadzi do rezultatu i co musi funkcjonować na poszczególnych etapach. Nie potrzebujesz od razu skomplikowanego programu do modelowania procesów. Kartka papieru, tablica lub prosty arkusz będą wystarczające, pod warunkiem że opiszesz rzeczywistą pracę, a nie oficjalną wizję tego, jak powinna wyglądać. Różnica bywa znaczna. W procedurze pracownik pobiera dane z centralnego systemu. W praktyce pobiera je z wiadomości przesyłanej codziennie przez koleżankę, która od pięciu lat wykonuje tę czynność, choć nikt nie wie dlaczego. Kiedy koleżanka zachoruje albo poczta przestanie działać, okazuje się, że organizacja odkryła nowy proces biznesowy. Szkoda tylko, że podczas awarii.