Adam Wojciechowski
Instytut Logistyki i Magazynowania

Wygrać konkurencję

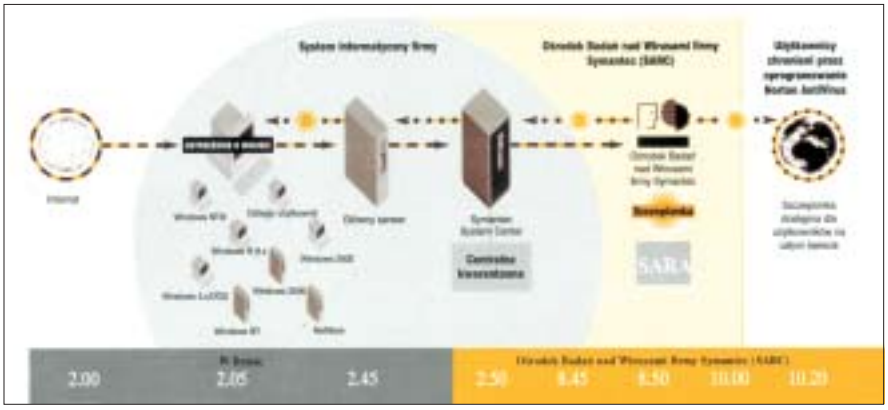
Na całym świecie widoczna jest stale postępująca globalizacja różnych dziedzin życia. Rynek stawia przed przedsiębiorstwami coraz wyższe wymagania w zakresie poziomu i efektywności obsługi klienta. Wysoka konkurencja na rynku wymusza na wszystkich działania mające na celu lepszą obsługę klienta. Wskazane jest, aby zadowolenie klienta spowodowało nawiązanie więzów partnerskich i wzajemnej lojalności. Lojalności klienta można oczekiwać tylko w sytuacji, kiedy osiągnięta zostanie najlepsza wzajemna relacja pomiędzy stronami, a to sprawia, że:

- wzrasta liczba zamówień, gdyż klient dostrzega duże zainteresowanie jego potrzebami i co ważniejsze, potrzeby te są w możliwie najwyższym stopniu zaspokajane
- dostawca uzyskuje poprawę wizerunku swojej firmy na rynku, w wyniku czego zyskuje nowych klientów, dla których jakość obsługi oraz otrzymywana tą drogą wartość dodana jest czynnikiem motywującym, skłaniającym do zakupu.

Osiągnięcie takiego poziomu możliwe jest tylko w wyniku wysokiego profesjonalizmu oraz perfekcyjnej logistycznie organizacji pracy, której jednym z istotnych ogniw jest przepływ informacji i dokumentów. Dynamiczny rozwój informatyki i telekomunikacji w latach osiemdziesiątych, wzbogacony o doświadczenia z prowadzonych prac wdrożeniowych, przyczynił się do szybkiego rozwoju różnych systemów w tym zakresie, a pojawienie się sieci internetowej spowodowało dalszy, jeszcze szybszy rozwój oferowanych rozwiązań. Wspólną cechą oferowanych systemów są elektronicznie realizowane funkcje:

- wymiany informacji (dokumentów) pomiędzy zarządzającymi, kompetentnymi działami, czy pracownikami przedsiębiorstwa
- nadzór i kontrola realizacji zleconych prac na dowolnym etapie obiegu dokumentów
- nadzór oraz kontrola czasu zarówno wykonania zleconych prac jak i obsługi klienta
- nadzór i kontrola przedstawicieli handlowych, również tych terenowych
- dokumentowanie wszelkich wykonywanych zadań
- ewidencjonowanie wszelkich zmian związanych z realizowanymi zadaniami
- dokumentowanie zawartych kontraktów oraz nadzór i kontrolę ich realizacji
- definiowanie hierarchii pracowników i obiegu dokumentów
- umożliwiające bieżącą i perspektywiczną analizę w zakresie zarejestrowanych informacji
- rejestrowanie informacji o nawiązanych kontaktach
- tworzenie zbiorów danych o klientach i ich oczekiwaniach.

Modułowa budowa oferowanych na rynku systemów informatycznej obsługi przepływu dokumentów pozwala na konfigurowanie dostosowane do logistycznych potrzeb zróżnicowanych profili działania wielu użytkowników. Jako przykłady wymienić można:



Rys. 1. Automatyczny cykl ochrony firmy Symantec

- **System Logotec DDM9000®** (*Document Data Managament*), w którego skład wchodzą cztery moduły funkcjonalne – Archiwum, Kontakt, Sprawy i Workflow.
- **System Obiegu Dokumentów NIL**, w którego skład wchodzą programy – Klienta (ANUBIS), Edycji Ścieżek (HORUS), Administracyjny (HORUS) i Baz danych.
- **System Zarządzania Dokumentami IDM** (*Integrated Document Managament*), w którego skład wchodzą moduły – Dokumentów (*Content Services*), Archiwum (*Image Services*), Automatyzacji procesu obiegu dokumentów (*WorkFlo Services*), Przeglądania i wyszukiwania (*IDM Desktop*), Przeglądarki internetowej (*WEB Services*), Projektowania procesów *(eProcess Services)*, Skanowania i zasilania archiwum (*Copture*), Raportowania (*Raport Manager*), Współpracy z aplikacjami klasy ERP (*Document Warehouse for ERP*) i Publikacji dokumentów poprzez strony www (*Web Publisher*).

Należy jednak pamiętać, że każdy z tych systemów powinien zostać zainstalowany w odpowiednio przygotowanym otoczeniu sieciowym. Wzajemne partnerstwo i wysoka konkurencja na rynku wymaga, aby instalacja posiadała szereg zabezpieczeń tak wewnątrz przedsiębiorstwa, jak też chroniących przed niebezpieczeństwami grożącymi z zewnątrz. W zakresie zabezpieczeń rynek oferuje wiele rozwiązań, których poziom funkcjonalny dostosowany jest do oczekiwań i możliwości finansowych zainteresowanego. Należy jednak w tym miejscu dokonać pewnego rozgraniczenia na zabezpieczenia przed:

- dostępem bezpośrednim (zagrożenie wewnętrzne) do wykorzystywanego w firmie sprzętu komputerowego
- dostępem do sieci komputerowej firmy z zewnątrz poprzez połączenie z siecią internetową
- utratą zgromadzonych w systemie zasobów informacyjnych i dokumentów.

Braki w zakresie zabezpieczeń doprowadzić mogą do:

- zniszczenia reputacji firmy
- strat finansowych

- bankructwa
- zagrożenia bezpieczeństwa życia.

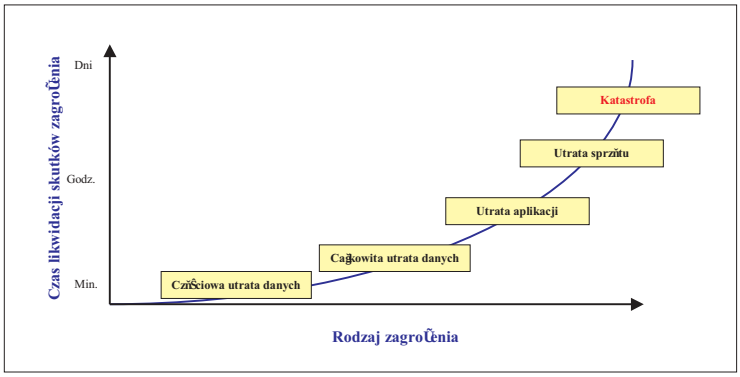
Przeprowadzone w świecie badania wykazały, że 80% przestępstw komputerowych dokonywanych jest w wyniku bezpośredniego (wewnętrznego) dostępu do zasobów sieci w firmie przez osoby nieuprawnione. W celu ograniczenia dostępu do sieci wewnątrz firmy nie wystarczające okazują się już identyfikatory dostępu i hasła. Na rynku oprócz różnych zabezpieczeń blokady typu SL (*System Lock*) oferowane są już rozwiązania wykorzystujące kontrolę dostępu za pomocą kart procesorowych czy identyfikację biometryczną, w której wykorzystywane są czujniki pojemnościowe odcisków palców. Dla zwiększenia bezpieczeństwa w praktyce stosowane są kombinacje różnych zabezpieczeń.

Upowszechnienie sieci komputerowych, a szczególnie Internetu, spowodowało duże zagrożenie dla zasobów zgromadzonych w systemach informatycznych firm przez różnego rodzaju stale rozwijane, skomplikowane wirusy. Mogą one zainfekować system w wyniku:

- przypadkowego przeniesienia wewnątrz firmy poprzez, np. zainfekowaną dyskietkę
- niespodziewanego, bezpośredniego lub pośredniego, świadomego działania z zewnątrz poprzez sieć internetową.

Zagrożenie to potęguje jeszcze bardziej możliwość ingerencji w ich zawartość lub utraty zasobów na rzecz konkurencji albo całkowitego zniszczenia, w wyniku świadomego oddziaływania z zewnątrz poprzez sieć internetową. Rynek w dziedzinie techniki IT prezentuje obecnie bogatą ofertę programów pozwalających na zabezpieczenie sieci użytkownika. Oprócz programów popularnych wykrywających i usuwających wykryte wirusy dostępne są programy inteligentne, o wysokim stopniu aktywności, chroniące sieć użytkownika przed zainfekowaniem na różnych jej platformach stacji roboczych oraz serwerów. W wyniku zastosowania zaawansowanych technologicznie automatycznych systemów ochrony antywirusowej uzyskać można duże prawdopodobieństwo bezawaryjnego funkcjonowania sieci. Przykład automatycznego cyklu ochrony firmy Symantec przedstawiono na rys. 1.

Poważnym zagrożeniem dla systemu przepływu informacji oraz dokumentu firmy jest utrata zgromadzonej w nim wiedzy o kontrahentach i realizowanych zadaniach, co może spowodować przerwanie ciągłości funkcjonowania przedsiębiorstwa. Kolejnym zagrożeniem są przypadki losowe (wyjątkowe), takie jak powódź, pożar itp. Najbardziej jaskrawym przykładem tego typu przypadków jest atak terrorystyczny, który miał miejsce w Stanach Zjednoczonych w dniu 11 wrześniu 2001 r. i jego konsekwencje. Rodzaje potencjalnych zagrożeń w stosunku do czasu ich likwidacji przedstawiono na rys. 2. Każda renomowana firma mając na uwadze różne możliwe przypadki utraty zasobów danych powinna posiadać „plan awaryjny". Powstanie takiego planu powinno być poprzedzone rozważeniem, jak może najlepiej zabezpieczyć zasoby przed sytuacjami wyjątkowymi.

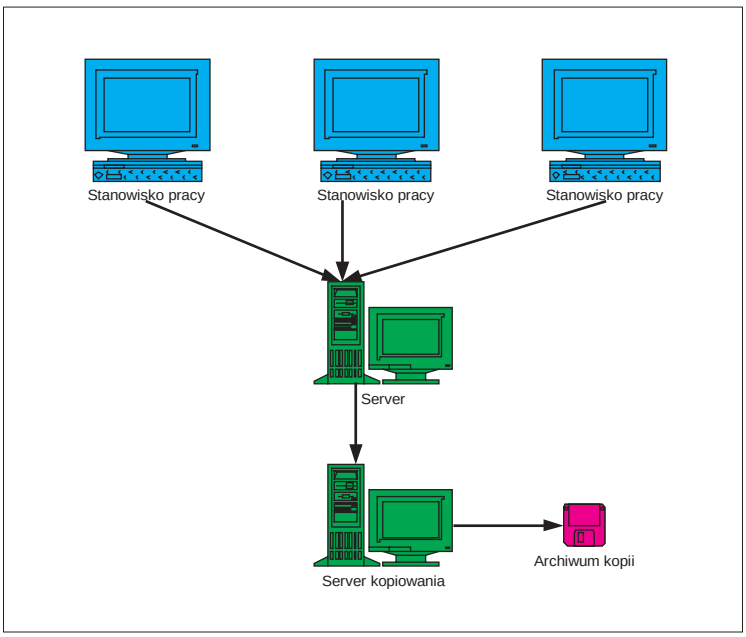


Rys. 2. Rodzaje potencjalnych zagrożeń a czas likwidacji ich skutków. *Źródło: Opracowanie własne*

Pewne jest, że każde przedsiębiorstwo, w którym ma prawidłowo funkcjonować informatyczny system zarządzania obiegiem informacji oraz dokumentów, musi systematycznie tworzyć kopie zapasowe – rys. 3, które pozwolą ograniczyć czas przerwy ciągłości funkcjonowania w sytuacjach awaryjnych i szybko przywrócić pełną sprawność działania. W tym zakresie rynek IT również ma dla zainteresowanych oferty o różnym poziomie zaawansowania technologicznego. Jako przykłady przytoczyć można:

- system tworzenia i zarządzania kopiami bezpieczeństwa LEGATO
- Oprogramowanie Tivoli Storage Managament.

Wskazane jest zwrócić jeszcze uwagę na fakt, że większość systemów zarządzania obiegiem informacji oraz dokumentów zawiera zbiory danych o klientach, które mogą zawierać dane osobowe, a te podlegają regulacjom prawnym określonym w Ustawie z dnia 29 sierpnia 1997 r. **o ochronie danych osobowych (Dz. U. 97.133.883** z późniejszymi zmianami). Ustawa ta określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane dotyczą. Jak widać ustawa obejmuje w praktyce wszystkie czynności na zbiorach zawierających dane osobowe, a to oznacza konieczność, z określonymi wyjątkami, ich rejestracji u Generalnego Inspektora Ochrony Danych Osobowych GIODO). Jednak, aby mogło dojść do rejestracji, spełnione muszą być przez administratora danych wymagania ustawowe. Trzeba sobie uczciwie powiedzieć, że jest ich dużo, a zgodnie z wykładnią prawną GIODO, niezależnie od tego czy zbiór podlega rejestracji czy nie, administratora danych obowiązany jest przestrzegać wszystkich przepisów określonych ustawą.



Rys. 3. Schemat tworzenia kopii zapasowych. *Źródło: Opracowanie własne*