Analiza i projektowanie

Analiza i projektowanie: Analiza wymagań systemowych i projektu do stworzenia systemu

Wprowadzenie

W kontekście wdrażania strategii konieczne są działania analityczne i projektowe w celu określenia potrzeb biznesowych i użytkowników systemu oraz opracowania planu jego budowy. W tej części omówiono nowe podejścia do analizy i projektowania wymagane dla systemów e-biznesu. Nie ma na celu wyjaśnienia, jak postępować zgodnie z dobrze ugruntowanymi technikami analizy i projektowania, takimi jak diagram przepływu danych, diagramy przepływu informacji i diagramowanie relacji encji. Opisywano je już wielokrotnie, na przykład w Bocij. Celem jest zapoznanie menedżerów z niektórymi technikami analizy i projektowania dla e-biznesu oraz zaznajomienie się z takimi technikami, jak analiza procesów, modelowanie danych i projektowanie przypadków użycia. Ta znajomość powinna pomóc we współpracy, gdy menedżerowie są zaangażowani w omawianie wymagań systemu z personelem technicznym.

Składa się z dwóch głównych części. W pierwszej części dokonujemy przeglądu technik analitycznych, a w szczególności analizy procesów pod kątem re-engineeringu, co jest ważne w wielu wdrożeniach e-biznesu. Dotykamy również modelowania danych. Modelowania danych nie opisano szczegółowo, ponieważ jest to bardzo dobrze znana technika. Druga część poświęcona jest projektowaniu systemów e-biznesu. Opisane techniki mają na celu poprawę jakości informacji użytkowników końcowych systemów e-biznesu - zapewnienie, że informacje są aktualne i bezpieczne, mają poprawną treść pod względem dokładności, trafności i kompletności oraz są w formie łatwej do interpretacji . Sekcja poświęcona projektowaniu architektonicznemu poświęcona jest integracji systemów w celu usprawnienia przepływu informacji, a także zapewnienia terminowego dostarczania informacji. Skoncentrowanie się na projektowaniu witryn zorientowanych na użytkownika pokazuje, jak za pomocą analizy przypadków użycia i wytycznych dotyczących projektowania interfejsu można tworzyć użyteczne systemy handlu elektronicznego po stronie sprzedającego lub kupującego o dobrej jakości informacji. Skoncentruj się na projektach zabezpieczeń, przeglądach wymagań bezpieczeństwa dla e-biznesu, przeglądach ogólnych podejść do bezpieczeństwa i wreszcie przyjrzymy się obecnemu wykorzystaniu technik bezpieczeństwa w handlu elektronicznym. Znaczenie analizy i projektowania jest takie, że nawet jeśli opracowano skuteczną strategię, jej wykonanie może zostać zniszczone przez nieskuteczną analizę i projektowanie.

Analiza dla e-biznesu: Wykorzystanie technik analitycznych do przechwytywania i podsumowania wymagania biznesowe i użytkownika.

Analiza dla e-biznesu

Analiza dla e-biznesu polega na zrozumieniu wymagań biznesowych i użytkowników dla nowego systemu. Typowe działania analityczne można podzielić na: zrozumienie bieżącego procesu, a następnie przegląd możliwych alternatyw dla wdrożenia rozwiązania e-biznesowego. W kolejnych sekcjach dokonamy przeglądu różnych technik, które pozwolą nam podsumować działanie obecnych procesów i proponowanych procesów e-biznesowych. W tej sekcji skupimy się na wykorzystaniu diagramów do przedstawienia procesów biznesowych. Analitycy zdają sobie sprawę, że dostarczanie wysokiej jakości informacji pracownikom i partnerom lub wymiana ich między procesami jest kluczem do budowania systemów informacyjnych, które poprawiają wydajność i obsługę klienta. Pant i Ravichandran mówią: Informacja jest czynnikiem koordynacji i kontroli i służy jako spoiwo, które spaja organizacje, franczyzy, łańcuchy dostaw i kanały dystrybucji. Oprócz przepływu materiałów i innych zasobów w każdej organizacji należy również efektywnie obsługiwać przepływ informacji. To pokazuje,

że w dobie e-biznesu analiza powinna być wykorzystywana jako narzędzie optymalizacji przepływu informacji zarówno wewnątrz, jak i na zewnątrz organizacji. W tym rozdziale zaczynamy od przyjrzenia się, jak zarządzanie przepływem pracy jest kluczem do zarządzania przepływami informacji opartymi na czasie. Następnie sprawdzamy, w jaki sposób modelowanie procesów jest wykorzystywane do analizy przepływów informacji w celu optymalizacji procesów biznesowych, a następnie analizujemy przechowywanie informacji poprzez krótki przegląd modelowania danych.

Zarządzanie przepływem pracy (WFM): automatyzacja przepływu informacji i zapewnia narzędzia do przetwarzania informacji zgodnie z zestawem reguł proceduralnych

Analiza i weryfikacja przepływu pracy organizacji w ramach zarządzania przepływem pracy (WFM) to koncepcja, która jest integralną częścią wielu aplikacji e-biznesowych, więc zanim przyjrzymy się technikom analizy procesów, przyjrzyjmy się, dlaczego przepływ pracy jest integralną częścią e-biznesu. WFM został zdefiniowany przez Koalicję Zarządzania Przepływem Pracy jako automatyzacja procesu biznesowego, w całości lub w części, podczas którego dokumenty, informacje lub zadania są przekazywane od jednego uczestnika do drugiego w celu podjęcia działania, zgodnie z zestawem reguł proceduralnych. Systemy przepływu pracy automatyzują procesy e-biznesu, zapewniając ustrukturyzowaną strukturę do obsługi procesu. Zastosowania przepływu pracy w e-biznesie obejmują zapytania dotyczące działań z zapytań klientów zewnętrznych lub zapytań wsparcia wewnętrznego. Zapytania te mogą być przesyłane pocztą elektroniczną, telefonicznie lub listownie. Zapytania e-mail mogą być analizowane i kierowane do właściwej osoby w zależności od ich tematu. Listy mogą wymagać zeskanowania przed dodaniem do kolejki przepływu pracy. Workflow pomaga zarządzać procesami biznesowymi, zapewniając priorytetyzację zadań do wykonania:

-> tak szybko, jak to możliwe

-> przez właściwych ludzi

-> we właściwej kolejności.

Podejście oparte na przepływie pracy zapewnia spójne, jednolite podejście do poprawy wydajności i lepszej obsługi klienta. Oprogramowanie workflow udostępnia funkcje do:

• przydzielać zadania ludziom

• przypominać ludziom o ich zadaniach, które są częścią kolejki workflow

• umożliwić współpracę między osobami dzielącymi się zadaniami

• odzyskać informacje potrzebne do wykonania zadania, takie jak dane osobowe klienta

• przedstawiać menedżerom przegląd statusu każdego zadania i wyników zespołu.

Jakie aplikacje workflow będą istnieć w firmie? W przypadku firmy B2B aplikacje e-biznesowe mogą obejmować:

1 Przepływ pracy administracyjnej. Dotyczy to wewnętrznych zadań administracyjnych. Przykłady obejmują zarządzanie zamówieniami zakupu oraz rezerwację wakacji i szkoleń.

2 Przepływy pracy. Są to przepływy pracy skierowane do klienta lub dostawcy. Przykładem przepływu pracy w produkcji jest oparta na intranecie i ekstranecie baza danych wsparcia klienta i system zarządzania zapasami zintegrowany z systemem dostawcy.

Noyes i Baber zwracają uwagę, że trudność w tego rodzaju dekompozycji procesu lub zadań polega na tym, że nie ma ustalonych reguł określających, jak nazwać różne poziomy dekompozycji, lub jak daleko

należy zdekomponować proces. Liczba poziomów i terminologia używana na różnych poziomach będą się różnić w zależności od używanej aplikacji i konsultanta, z którym możesz pracować. Georgakoupoulos i inni mówią o zagnieżdżaniu zadań w podziale na podzadania jako części opartej na aktywności metody opisu przepływów pracy. Podają przykład procesu przepływu pracy dla zamówień, w którym zadanie „przygotowanie materiałów" jest dalej podzielone na podzadania o statusie „Sprawdź status", uzyskaj oferty "i„ złóż zamówienie ". Curtis przedstawia przydatne ramy, odnosząc się do jednostek lub elementów procesu na każdym poziomie procesu w następujący sposób:

Proces biznesowy poziomu 1 rozkłada się na:

Działania poziomu 2, które są dalej podzielone na:

Zadania poziomu 3 i wreszcie:

Zadania podrzędne poziomu 4.

Próby ujednolicenia znaczenia tych terminów zostały podjęte przez Koalicję Zarządzania Przepływem Pracy, organizację zajmującą się normami branżowymi, która opisuje różne elementy procesu w następujący sposób:

1 Proces biznesowy. Zestaw jednej lub więcej powiązanych procedur lub czynności, które wspólnie realizują cel biznesowy lub cel polityki, zwykle w kontekście struktury organizacyjnej definiującej role i relacje funkcjonalne.

2 Aktywność Opis pracy, która stanowi jeden logiczny krok w procesie. Działanie może być działaniem ręcznym, które nie obsługuje automatyzacji komputera lub działaniem (zautomatyzowanym) przepływu pracy. Działanie przepływu pracy wymaga zasobów ludzkich i / lub maszynowych do obsługi wykonywania procesu; tam, gdzie wymagane są zasoby ludzkie, działanie jest przydzielane uczestnikowi przepływu pracy.

3 Element pracy Przedstawienie pracy do przetworzenia (przez uczestnika przepływu pracy) w kontekście działania w ramach instancji procesu. Działanie zazwyczaj generuje jeden lub więcej elementów pracy, które razem stanowią zadanie do wykonania przez użytkownika (przepływ pracy uczestnika) w ramach tego działania.

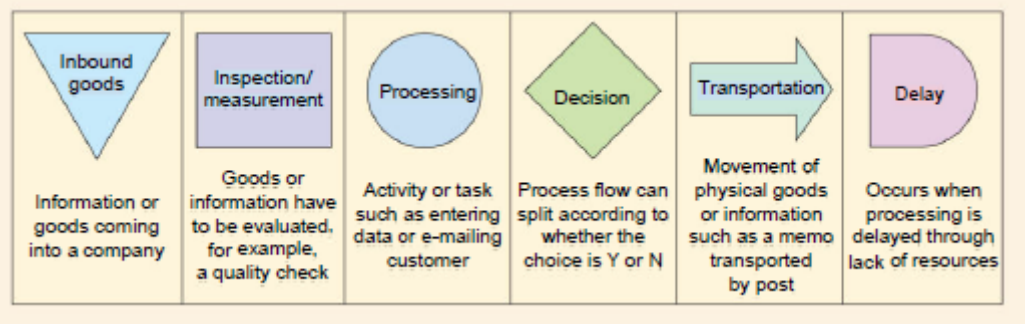
Zależności procesów

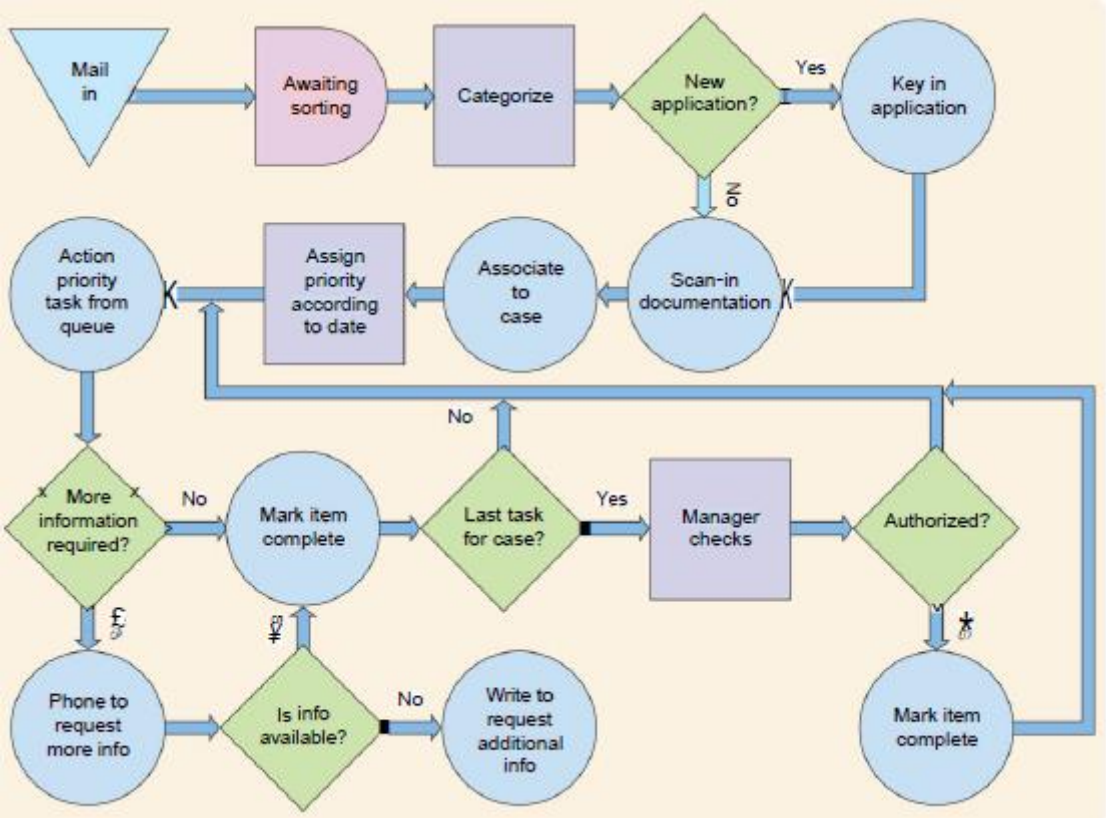
Zależności procesów podsumowują kolejność, w jakiej zachodzą działania, zgodnie z regułami biznesowymi rządzącymi procesami. Zwykle działania są sekwencyjne i mają charakter seryjny; czasami działania mogą zachodzić jednocześnie, gdy są znane jako równoległe. Diagramy przepływu danych i schematy blokowe są szeroko stosowane jako techniki tworzenia diagramów w celu pokazania zależności procesów. W tej sekcji omówimy trzy techniki pokazywania zależności, które są częściej stosowane w analizie e-biznesu. Są to schematy procesów przepływu i diagramy sieciowe, w tym standard EPC (łańcuch procesów sterowany zdarzeniami) używany przez produkt SAP.

Wykresy procesu

Prosty schemat blokowy jest dobrym punktem wyjścia do opisu sekwencji działań przepływu pracy będącego częścią procesu e-biznesowego. Pomimo swojej prostoty schematy blokowe są skuteczne, ponieważ są łatwe do zrozumienia dla personelu nietechnicznego, a także wskazują na wąskie gardła i nieefektywność. Schematy procesów są powszechnie używane podczas rozwiązywania problemów w e-biznesie, zarówno w biurze, jak i na zapleczu. Każdy symbol na wykresie odnosi się do konkretnego

działanie w ramach całego procesu. Objaśnienie symboli używanych w analizie schematu procesu przedstawiono na rysunku .





Analiza czasu trwania wysiłku

Analiza czasu trwania wysiłku to narzędzie analityczne, którego można użyć do obliczenia ogólnej wydajności procesu, gdy przeprowadziliśmy szczegółową analizę. Aby to zrobić, sumujemy średni czas potrzebny pracownikom na wykonanie każdej czynności składającej się na cały proces, a następnie dzielimy go przez całkowity czas trwania całego procesu. Całkowity czas procesu jest często znacznie dłuższy, ponieważ obejmuje to czas, gdy zadanie nie jest wykonywane. Tutaj dzieje się to podczas transportu formularzy oraz kiedy czekają na tacach wyjściowych i tacach. Zależność efektywności można podać jako:

Wydajność = X (T (nakłady wysiłkowe)) / T (całkowity czas procesów)

Jeśli zastosujemy analizę czasu trwania wysiłku do pierwszego scenariusza, gdzie opóźnienia i transport nie przyczyniają się do całego procesu, zobaczymy, że wydajność tego niezwykle nieefektywnego procesu wynosi zaledwie 2 procent! Środek ten można rozszerzyć, odnotowując czynności, które dodają wartość dla klienta, a nie tylko czynności administracyjne.

Diagramy sieciowe

Chociaż diagramy przepływu danych i schematy procesów przepływu danych mogą dobrze wskazywać kolejność, w jakiej występują czynności i zadania, często nie dają wystarczająco ścisłej, formalnej definicji sekwencji procesu niezbędnej do wprowadzenia danych do e-biznesu, przepływu pracy lub ERP system. Aby to zrobić, możemy użyć diagramu sieciowego znanego jako GAN (uogólniona sieć aktywności). Tutaj węzły są dodawane między ramkami reprezentującymi zadania, aby precyzyjnie zdefiniować alternatywy które istnieją po zakończeniu zadania. Najczęstszą sytuacją jest to, że jedno działanie musi następować po drugim, na przykład po sprawdzeniu tożsamości klienta musi nastąpić sprawdzenie zdolności kredytowej. Tam, gdzie istnieją alternatywy, logika jest zdefiniowana w węźle w następujący sposób: gdzie a pojedyncza ścieżka pochodzi z dwóch lub więcej alternatyw, węzeł definiuje się jako węzeł OR, a gdy można podążać kilkoma ścieżkami, jest to węzeł AND. Węzły łączone łączą poprzednie czynności, a podziały określają, które działania będą następować. Tam, gdzie istnieją alternatywy, reguły biznesowe definiuje się jako warunki wstępne lub warunki końcowe.

Model łańcucha procesów sterowanych zdarzeniami (EPC)

Jedną z najczęściej stosowanych metod opisu zdarzeń i procesów biznesowych jest metoda łańcucha procesów sterowana zdarzeniami (EPC). Zostało to spopularyzowane poprzez zastosowanie go do re-engineeringu przedsiębiorstw przy użyciu produktu SAP R / 3 ERP, którego sprzedaż na świecie wynosi kilka miliardów dolarów. Ponad 800 standardowych biznesowych EPC zostało zdefiniowanych do obsługi systemu SAP R / 3; mają one na celu jasne zilustrowanie reguł biznesowych do interpretacji przez użytkowników biznesowych przed wprowadzeniem ich do oprogramowania. Różne elementy modelu EPC przedstawiono w tabeli 11.5; Obejmują one różne typy zależności, które omówiono wcześniej w tabeli 11.4. Rysunek 11.4 to meta-model EPC ilustrujący, w jaki sposób różne elementy są ze sobą powiązane. Ten rysunek przedstawia, w jaki sposób funkcje biznesowe są wyzwalane przez transakcje na obiektach biznesowych, które również prowadzą do zdarzenia biznesowego. Przepływy sterowania łączą czynności, zdarzenia i operatory logiczne. Jednostki lub obiekty informacyjne to elementy, takie jak zamówienia sprzedaży lub faktury.

Walidacja nowego modelu procesu

Niezależnie od tego, która metoda została użyta do ustalenia definicji procesu, musimy sprawdzić, czy definicja procesu jest realistyczna. Podczas opracowywania listy życzeń dotyczących możliwości procesu i odpowiednich biznes rządzi etapami opisanymi przez Davida Taylora w jego książce o inżynierii współbieżnej. Sugeruje, że po ustanowieniu nowych procesów są one sprawdzane pod kątem normalności poprzez przeprowadzenie rozmowy, przejścia i przejścia". W tym miejscu zespół projektowy opisze proponowany proces biznesowy jako model, w którym różne obiekty biznesowe oddziałują na siebie, a na etapie omówienia będą przeprowadzać różne scenariusze biznesowe przy użyciu kart do opisywania obiektów i usług, które dostarczają innym obiektom biznesowym. Po dostosowaniu modelu etap przejścia obejmuje bardziej szczegółowy scenariusz, a zespół projektowy odegra role w usługach świadczonych przez obiekty. Ostatnim etapem jest sprawdzenie jakości, w którym nie następuje debugowanie na miejscu - opisane są tylko interakcje między obiektami. Coraz częściej wykorzystuje się oprogramowanie symulacyjne do modelowania alternatywnych scenariuszy.

Encja: grupa powiązanych danych, takich jak jednostka klienta, zaimplementowana jako tabela.

Tabela bazy danych: Każda baza danych zawiera kilka tabel.

Atrybut: właściwość lub cecha jednostki zaimplementowana jako pole.

Pole: atrybuty produktów, takie jak data urodzenia

Rekord: zbiór pól dla jednego wystąpienia jednostki, na przykład Customer Smith.

Relacja: opisuje sposób łączenia różnych tabel.

Klucz podstawowy: pole, które jednoznacznie identyfikuje każdy rekord w tabeli.

Klucz dodatkowy: pole używane do łączenia tabel przez połączenie z kluczem podstawowym w innej tabeli.

Modelowanie danych

Modelowanie danych w systemach e-biznesu i handlu elektronicznego wykorzystuje ugruntowane techniki, takie jak normalizacja, które są wykorzystywane do analizy i projektowania relacyjnych baz danych. W konsekwencji, ta sekcja jest krótka w porównaniu z sekcją dotyczącą modelowania procesów, która wprowadza kilka nowych technik. W tej sekcji podano kilka podstawowych definicji jako przypomnienie kluczowych terminów. Zanim zaczniemy, warto wspomnieć, że pojawienie się eksploracji danych i podejść obiektowych oznaczało zwiększenie wykorzystania nierelacyjnych projektów baz danych. Podejście, którego używamy do eksploracji modelowania danych w handlu elektronicznym, polega na wykorzystaniu przykładów identyfikujących typowe elementy modelowania danych dla systemu handlu elektronicznego po stronie sprzedawcy. Będziemy używać modelowania ER (relacji jednostek) do przeglądu typowych struktur dla tych baz danych. W prostym modelowaniu ER istnieją trzy główne etapy.

1 Zidentyfikuj podmioty

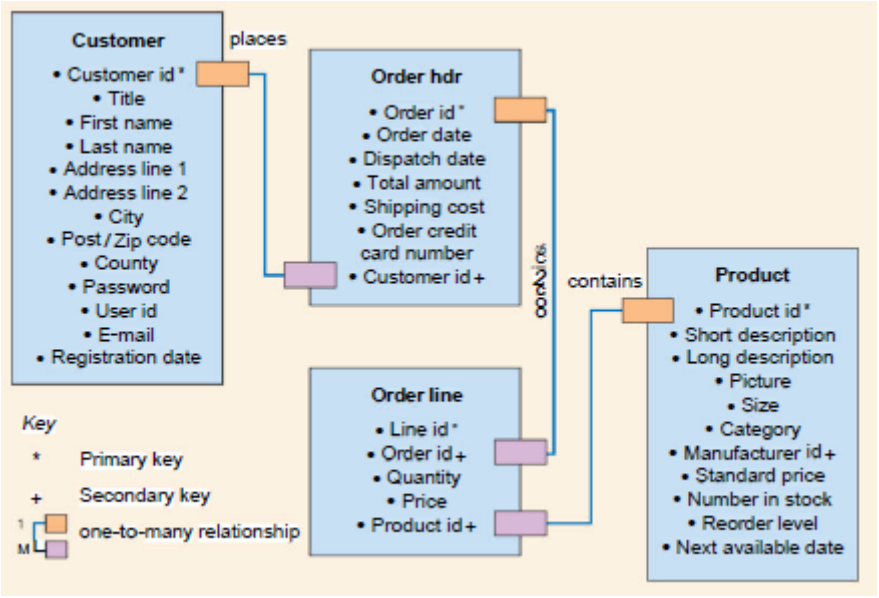
Podmioty definiują szerokie grupy informacji, takie jak informacje o różnych osobach, transakcjach lub produktach. Przykłady obejmują klientów, pracowników, zamówienia sprzedaży, zamówienia. Po wdrożeniu projektu każdy projekt utworzy tabelę bazy danych.

2 Zidentyfikuj atrybuty jednostek

Jednostki mają różne właściwości zwane „atrybutami", które opisują cechy każdej pojedynczej instancji jednostki. Na przykład jednostka klienta ma takie atrybuty, jak imię i nazwisko, numer telefonu i adres e-mail. Po wdrożeniu projektu każdy atrybut utworzy pole, a zbiór pól dla jednej instancji jednostki, takiej jak określony klient, utworzy rekord.

3 Zidentyfikuj relacje między podmiotami

Relacje między jednostkami wymagają określenia, które pola są używane do łączenia tabel. Na przykład w przypadku każdego zamówienia składanego przez klienta musimy wiedzieć, który klient złożył zamówienie i jaki produkt zamówił. Jak widać na rysunku



, pola identyfikatora klienta i identyfikatora produktu służą do powiązania informacji o zamówieniu między trzema tabelami. Pola używane do łączenia tabel nazywane są „polami kluczowymi". Klucz podstawowy służy do jednoznacznego identyfikowania każdego wystąpienia jednostki, a klucz pomocniczy służy do łączenia z kluczem podstawowym w innej tabeli. Na rysunku kluczem podstawowym tabeli klientów jest identyfikator klienta, ale pole identyfikatora klienta w tabeli zamówień jest tutaj kluczem pomocniczym, który łączy się z tabelą klientów. Ta relacja jest przykładem relacji jeden do wielu, ponieważ każdy klient może złożyć wiele zamówień przez cały okres trwania relacji. Normalizacja jest dodatkowym etapem, nieuwzględnionym tutaj, służącym do optymalizacji bazy danych w celu zminimalizowania redundancji lub powielania informacji.

Projekt systemu: określa sposób działania systemu informacyjnego.

Model klient-serwer: architektura systemu, w której komputery użytkowników końcowych, takie jak komputery osobiste, zwane „klientami", uruchamiają aplikacje podczas uzyskiwania dostępu do danych i prawdopodobnie programów z serwera.

Serwer klientów trójwarstwowy: pierwsza warstwa to klient obsługujący wyświetlanie, drugi to logika aplikacji i reguły biznesowe, trzeci to przechowywanie bazy danych.

Cienki klient: urządzenie dostępu użytkownika końcowego (terminal), w którym wymagania obliczeniowe, takie jak przetwarzanie i przechowywanie (a tym samym koszty), są zminimalizowane

Projekt dla e-biznesu

Element projektowy tworzenia systemu e-biznesowego obejmuje określenie struktury systemu. W dwóch kolejnych sekcjach Focus on przyjrzymy się dwóm aspektom projektowania, które są bardzo ważne znaczenie postrzegania systemów e-biznesu przez klientów - bezpieczeństwo i projektowanie interfejsów. Wcześniej rozważamy ogólny projekt architektoniczny systemów e-biznesu.

Projekt architektoniczny systemów e-biznesu

Punktem wyjścia do projektowania systemów e-biznesu jest zapewnienie istnienia wspólnej architektury w całej firmie pod względem technologii sprzętu i oprogramowania, aplikacji i procesów biznesowych. Systemy e-biznesu opierają się na tej samej architekturze modelu klient-serwer, co wiele biznesowych systemów informacyjnych stworzonych w latach 90. W przypadku e-biznesu klientami są

zazwyczaj pracownicy, dostawcy lub komputery stacjonarne klientów, które stanowią „front-end” punkt dostępu do aplikacji e-biznesowych. Klienci są podłączeni do serwera „zaplecza” przez intranet, ekstranet lub Internet. W Częściach 3 i 6 omówiliśmy kwestie zarządzania związane z wyborem systemów e-biznesu typu „oprogramowanie jako usługa” (SaaS), które są systemami klient-serwer, w których klient jest przeglądarką internetową na komputerze lub urządzeniu mobilnym, a serwer jest zlokalizowany poza organizacją, a proces składania wniosków jest często współdzielony z wieloma innymi firmami w modelu „multi-tenancy”. Kluczową decyzją projektową w systemach klient-serwer jest rozkład różnych zadań związanych z dostarczaniem działającej aplikacji użytkownikom między klientem a serwerem. Typowa sytuacja dla tych zadań w systemie e-biznesu to:

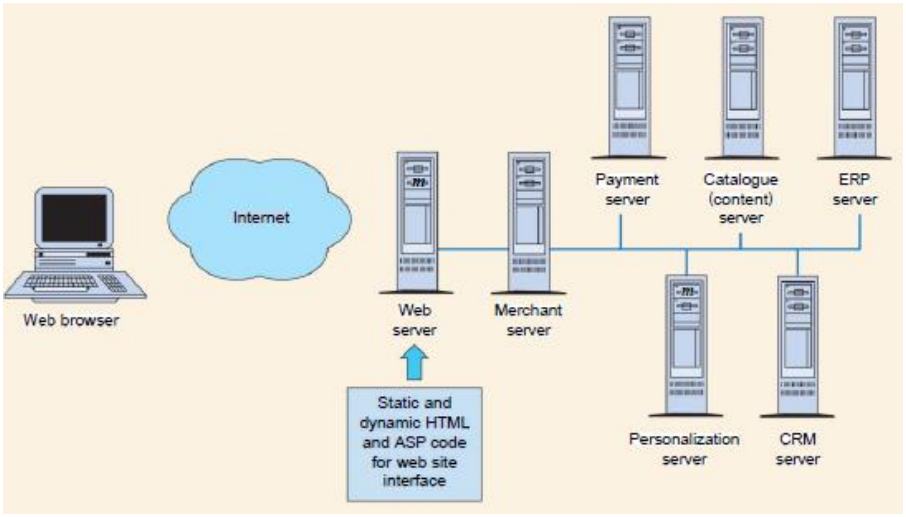
• Przechowywanie danych. Głównie na serwerze. Idealnie ogranicza się przechowywanie klientów do plików cookie służących do identyfikacji użytkowników i śledzenia sesji. Identyfikatory plików cookie dla każdego użytkownika systemu są następnie powiązane z danymi użytkownika, które są przechowywane na serwerze bazy danych.

• Przetwarzanie zapytań. Przeważnie na serwerze, chociaż na kliencie można przeprowadzić pewną weryfikację.

• Wyświetlacz. Jest to w dużej mierze funkcja klienta.

• Logika aplikacji. Tradycyjnie we wczesnych aplikacjach PC była to funkcja klienta, ale w przypadku systemów e-biznesu celem projektu jest maksymalizacja przetwarzania logiki aplikacji, w tym reguł biznesowych na serwerze.

Typowa architektura e-biznesu wykorzystuje trójwarstwowy model klient-serwer, w którym klient jest używany głównie do wyświetlania z logiką aplikacji i regułami biznesowymi podzielonymi na partycje na serwerze, który jest drugą warstwą, a serwer bazy danych jest trzecią warstwą. Ponieważ większość przetwarzania jest wykonywana na serwerach, a nie na kliencie, architektura ta jest czasami nazywana „cienkim klientem”, ponieważ rozmiar programu wykonywalnego jest mniejszy. Dostawca serwera aplikacji (ASP) opisany w rozdziale 3 jest zwykle oparty na modelu trójwarstwowym. Chociaż trójwarstwowy model systemu e-biznesu sugeruje stosunkowo prosty projekt architektoniczny, rzeczywistość jest bardziej złożona. Potrzebne są różne serwery, które łączą logikę aplikacji i pamięć bazy danych dla różnych wymagań. Mogą to być fizycznie oddzielne serwery lub mogą być połączone. Rysunek przedstawia typową architekturę e-biznesu.



Przeznaczenie każdego z serwerów jest następujące:

• Serwer sieci Web. Zarządza żądaniami HTTP od klienta i działa jako pasywny broker dla innych serwerów. Zwraca lub wyświetla strony internetowe.

• Serwer handlowy. Jest to główna lokalizacja logiki aplikacji i integruje całą aplikację poprzez wysyłanie żądań do innych komponentów serwera.

• Serwer personalizacji. Zapewnia dostosowaną zawartość - może być częścią funkcjonalności serwera handlowego.

• Serwer płatności. Zarządza systemami płatności i zabezpiecza transakcje.

• Serwer katalogów. Serwer zarządzania dokumentami używany do wyświetlania szczegółowych informacji o produkcie i specyfikacji technicznych.

• Serwer CRM. Przechowuje informacje o wszystkich kontaktach z klientami.

• Serwer ERP. Wymagane do informacji o dostępności zapasów i cenach od klienta.

Konieczny będzie również dostęp do przetwarzania i historii zamówień sprzedaży. Logistyka dystrybucji będzie również zorganizowana przez serwer ERP.

Projekt zorientowany na użytkownika: projekt oparty na optymalizacji doświadczenia użytkownika pod kątem wszystkich czynników, w tym interfejsu użytkownika, które na to wpływają.

Projekt witryny zorientowany na użytkownika

Ponieważ systemy e-biznesu są często systemami skierowanymi do klientów lub pracowników, znaczenie interakcji człowiek-komputer jest duże w projektowaniu aplikacji internetowych. Odnosząc się do projektowania witryn internetowych, Nigel Bevan mówi: Jeśli witryna internetowa nie spełnia potrzeb zamierzonych użytkowników, nie będzie odpowiadać potrzebom organizacji, która ją udostępnia. Tworzenie witryny sieci Web powinno koncentrować się na użytkowniku i oceniać ewoluujący projekt pod kątem wymagań użytkownika. Noyes i Baber wyjaśniają, że projektowanie zorientowane na użytkownika to coś więcej niż projektowanie interfejsu użytkownika. Można to sobie wyobrazić jako skupiające się na człowieku, ale otoczone koncentrycznie przez czynniki wpływające na użyteczność, takie jak interfejs użytkownika, komputery, miejsce pracy i środowisko. Tutaj przyjrzymy się konkretnie interfejsowi użytkownika. Projektowanie zorientowane na użytkownika rozpoczyna się od zrozumienia natury i zróżnicowania w obrębie grup użytkowników. Według Bevana kwestie do rozważenia obejmują:

* Kim są ważni użytkownicy?

* Jaki jest ich cel w dostępie do witryny?

* Jak często będą odwiedzać witrynę?

* Jakie mają doświadczenie i wiedzę?

*Jakiej są narodowości? Czy potrafią czytać po angielsku?

* Jakiego rodzaju informacji szukają?

* W jaki sposób będą chcieli wykorzystać informacje: przeczytać je na ekranie, wydrukować lub pobrać?

* Z jakiego typu przeglądarek będą korzystać? Jak szybkie będą ich łącza komunikacyjne?

* Jak dużego ekranu / okna będą używać, z iloma kolorami?

Wrażenia klientów online: połączenie racjonalnych i emocjonalnych czynników związanych z korzystaniem z usług online firmy, które wpływają na postrzeganie marki przez klientów w internecie.

Zanim przeanalizujemy najlepsze praktyki w projektowaniu zorientowanym na użytkownika, należy zauważyć, że użyteczność i dostępność to tylko część ogólnego doświadczenia, które determinuje wrażenia odwiedzającego. W Części 5, w części poświęconej roli brandingu w ramach element miksu Produkt, wyjaśniliśmy, jak ważne jest, aby zapewnić klientom obietnicę tego, co reprezentacja marki w Internecie zapewni klientom. Koncepcja obietnicy marki online jest ściśle związana z koncepcją zapewniania obsługi klienta online. W tej części omówimy różne praktyczne działania, które firmy mogą podjąć, aby stworzyć i utrzymać satysfakcjonujące doświadczenia online. Alison Lancaster, ówczesna szefowa marketingu i katalogów w John Lewis Direct, a obecnie dyrektor ds. Marketingu w Charles Tyrrwhit (www.ctshirts.co.uk), wskazuje na wysiłek potrzebny do stworzenia klienta centralnej obecności w Internecie, który mówi: : Dobra witryna powinna zawsze zaczynać się od użytkownika. Dowiedz się, kim jest klient, jak korzysta z kanału do robienia zakupów i jak działa rynek w tej kategorii. Obejmuje to zrozumienie, kim są Twoi konkurenci i jak działają w Internecie. Potrzebujesz ciągłych badań, opinii i testów użyteczności, aby nadal monitorować i rozwijać doświadczenia klientów online. Klienci chcą wygody i łatwości składania zamówień. Chcą witryny, którą można szybko pobrać, dobrze zorganizowaną i łatwą w nawigacji. Jak widać, tworzenie skutecznych doświadczeń online jest wyzwaniem, ponieważ istnieje wiele praktycznych kwestii do rozważenia, który opiera się na diagramie autorstwa de Chernatony, który zasugerował, że dostarczanie doświadczeń online obiecanych przez markę wymaga dostarczanie racjonalnych wartości, wartości emocjonalnych i obiecanych doświadczeń (opartych na wartościach racjonalnych i emocjonalnych). Czynniki, które wpływają na doświadczenia klientów online, można przedstawić w formie piramidy czynników sukcesu, (różne czynniki sukcesu odzwierciedlają aktualne najlepsze praktyki i różnią się od tych z de Chernatony). Diagram podkreśla również znaczenie dostarczania jakości usług online, na co wskazują Trocchia i Janda. Badania przeprowadzone przez Christodoulides i inni przetestowali znaczenie szeregu wskaźników wartości marki online dla internetowych firm zajmujących się sprzedażą detaliczną i usługami. Analiza ta została przeprowadzona w odniesieniu do tych pięciu wymiarów wartości marki, ocenianych poprzez zadawanie pytań, które są wymienione poniżej, ponieważ zapewniają one doskonałe ramy, które można zastosować do oceny i porównania jakości doświadczenia marki w różnych typach witryn internetowych:

1 Połączenie emocjonalne

P: Czuję się związany z typem ludzi, którzy są klientami [X]

P2: 1 czuję, że [X] naprawdę się o mnie troszczy

P3: 1 czuję, że [X] naprawdę mnie rozumie

2 Doświadczenie online

P4: Witryna internetowa [X] zapewnia łatwe do naśladowania ścieżki wyszukiwania

P5: 1 nigdy nie czuć się zagubionym podczas przeglądania witryny internetowej [X]

P6: 1 udało mi się uzyskać potrzebne informacje bez żadnych opóźnień

3 Elastyczny charakter obsługi

P7: [X] jest chętny i gotowy do odpowiedzi na potrzeby klientów

P8: Witryna internetowa firmy [X] umożliwia odwiedzającym „rozmowę zwrotną5 z [X]”

4 Zaufaj

P9: 1 ufam firmie [X], że moje dane osobowe będą bezpieczne

Ql0: 1 Bezpieczne transakcje z [X]

5 Spełnienie

Qll: Mam to, co zamówiłem w witrynie internetowej [X]

P12: Produkt został dostarczony w terminie obiecanym przez [X]

Użyteczność: podejście do projektowania witryn internetowych mające na celu umożliwienie wykonywania zadań użytkownika.

Recenzja eksperta: analiza istniejącej witryny lub prototypu przeprowadzona przezdoświadczonego eksperta w dziedzinie użyteczności, który na podstawie swojej wiedzy na temat zasad projektowania stron internetowych i najlepszych praktyk zidentyfikuje braki i ulepszenia witryny.

Testowanie użyteczności / użytkownika: obserwuje się działanie reprezentatywnych użytkowników reprezentatywne zadania za pomocą systemu.

Użyteczność

Użyteczność to kluczowa koncepcja w projektowaniu zorientowanym na użytkownika, która jest stosowana do analizy i projektowania szeregu produktów, co określa ich łatwość w użyciu. Norma ISO British Standards Institute: Human-Centred Design Processes for Interactive Systems definiuje użyteczność jako: stopień, w jakim produkt może być używany przez określonych użytkowników do osiągnięcia określonych celów ze skutecznością, wydajnością i satysfakcją w określonym kontekście użytkowania. Możesz zobaczyć, jak łatwo można zastosować tę koncepcję do projektowania witryn internetowych - odwiedzający często mają zdefiniowane cele, takie jak znalezienie określonych informacji lub wykonanie czynności, takiej jak rezerwacja lotu lub sprawdzenie salda konta. W klasycznej książce Jakoba Nielsena, Designing Web Usability , opisuje on użyteczność w następujący sposób: Inżynierskie podejście do projektowania witryn internetowych, mające na celu zapewnienie łatwości do nauczenia się interfejsu użytkownika, łatwego do zapamiętania, bezbłędności, wydajności i satysfakcji użytkownika. Obejmuje testy i ocenę, aby zapewnić jak najlepsze wykorzystanie nawigacji i łączy w celu uzyskania dostępu do informacji w jak najkrótszym czasie. Proces towarzyszący architekturze informacji. W praktyce użyteczność obejmuje dwa kluczowe działania projektowe. Przeglądy eksperckie są często przeprowadzane na początku projektu przeprojektowania w celu zidentyfikowania problemów z poprzednim projektem. Testy użyteczności obejmują:

1 Identyfikacja reprezentatywnych użytkowników serwisu i typowych zadań;

2 Poproszenie ich o wykonanie określonych zadań, takich jak znalezienie produktu lub sfinalizowanie zamówienia;

3 Obserwowanie tego, co robią i jak im się to udaje.

Aby witryna odniosła sukces, należy wykonać zadania lub czynności użytkownika:

• Specjaliści ds. Użyteczności sieci skutecznie mierzą ukończenie zadania, na przykład tylko 3 na 10 odwiedzających witrynę internetową może być w stanie znaleźć numer telefonu lub inną informację.

• Wydajnie - specjaliści ds. Użyteczności sieciowej mierzą również, ile czasu zajmuje wykonanie zadania na stronie lub liczbę kliknięć, które trzeba wykonać.

Jakob Nielsen najlepiej wyjaśnia imperatyw użyteczności w swoim „Usability 101" (www.useit.com/ alertbox / 20030825.html). On mówi:

W sieci użyteczność jest niezbędnym warunkiem przetrwania. Jeśli strona internetowa jest trudna w obsłudze, ludzie ją opuszczają. Jeśli strona główna nie określa jasno, co oferuje firma i co użytkownicy mogą robić w witrynie, ludzie opuszczają witrynę. Jeśli użytkownicy zgubią się w witrynie, odchodzą. Jeśli informacje w witrynie są trudne do odczytania lub nie zawierają odpowiedzi na kluczowe pytania użytkowników, opuszczają ją. Zwróć uwagę na wzór? Z tych powodów Nielsen sugeruje, że około 10% budżetu projektu projektowego powinno być przeznaczone na użyteczność, ale często rzeczywiste wydatki są znacznie mniejsze.

Ocena projektów

Test efektywnego projektowania pod kątem użyteczności jest według Bevana zależny od trzech obszarów:

1 Skuteczność - czy użytkownicy mogą poprawnie i kompletnie wykonywać swoje zadania?

2 Produktywność (efektywność) - czy zadania są wykonywane w akceptowalnym czasie?

3 Satysfakcja - czy użytkownicy są zadowoleni z interakcji?

Modelowanie przypadków użycia: podejście do systemu modelowania zorientowane na wymagania użytkownika.

Unified Modeling Language (UML): język używany do określania, wizualizacji i dokumentowania artefaktów systemu zorientowanego obiektowo.

Personas projektowania stron internetowych: podsumowanie cech, potrzeb, motywacji i środowiska typowych użytkowników strony internetowej.

Primary persona: reprezentacja typowego użytkownika witryny, który ma strategiczne znaczenie dla skuteczności witryny, ale którego potrzeby trudno jest spełnić.

Scenariusze klientów (ścieżki użytkownika): alternatywne zadania lub wyniki wymagane przez użytkownika witryny internetowej. Zazwyczaj realizuje się w serii etapów różnych zadań obejmujących różne potrzeby informacyjne lub doświadczenia.

Analiza przypadków użycia

Metoda przypadków użycia analizy i modelowania procesów została opracowana na początku lat 90. XX wieku w ramach rozwoju technik obiektowych. Jest to część metodologii znanej jako „Unified Modeling Language" (UML), która stara się ujednolicić podejścia, które ją poprzedzały, takie jak notacje Booch, OMT i Objectory. Jacobsen i in. (1994) podają przystępne wprowadzenie i opisują, w jaki sposób modelowanie obiektów można zastosować do analizy przepływu pracy.

Analiza persona i scenariuszy

Projektanci witryn internetowych i specjaliści ds. marketingu używają podobnego modelu do przypadku użycia przy projektowaniu witryn internetowych, preferowanego przez analityków i projektantów systemów, ale przy użyciu innej terminologii. Marketerzy tworzą projekty stron internetowych dla typowych odwiedzających witrynę; jest to potężna technika wpływania na

planowanie kampanii online oraz użyteczność i zorientowanie na klienta witryny internetowej. Forrester zbadał wykorzystanie person i odkrył, że badacze etnograficzni przeprowadzili średnio 21 wywiadów z typowymi użytkownikami na projekt, przy czym średnio od czterech do ośmiu osób, a ten koszt wynosił od 47 000 do 500 000 $! Przykładem może być Ford, który używa trzech osób kupujących na Ford.com. Ich „główna osobowość" „Marie" - dopiero zaczyna proces zakupu samochodu, nie zdecydowała się na markę, nie wie o samochodach i potrzebuje pomocy. Staples.com ma siedem person dla kupujących, a Microsoft siedem dla Windows XP. Personas to w zasadzie „miniatura" opisu typu osoby. Były używane przez długi czas w badaniach do segmentacji i reklamy, ale w ostatnich latach okazały się również skuteczne w ulepszaniu projektowania witryn internetowych przez firmy, które zastosowały tę technikę. Scenariusze klientów są opracowywane dla różnych osób. Patricia Seybold w książce The Customer Revolution wyjaśnia je w następujący sposób: Scenariusz klienta to zestaw zadań, które dany klient chce lub musi wykonać, aby osiągnąć pożądany rezultat. Zobaczysz, że można opracować scenariusze dla każdej persony. W przypadku banku internetowego scenariusze mogą obejmować:

1 Nowy klient - otwarcie konta internetowego

2 Istniejący klient - przeniesienie konta online

3 Istniejący klient - znalezienie dodatkowego produktu.

Każdy scenariusz jest podzielony na serię kroków lub zadań przed ukończeniem scenariusza. Najlepiej potraktować te kroki jako serię pytań, które zadaje odwiedzający. Poprzez identyfikację pytań projektanci witryn internetowych identyfikują różne potrzeby informacyjne różnych typów klientów na różnych etapach procesu zakupu. Korzystanie ze scenariuszy jest prostą, ale bardzo skuteczną techniką projektowania witryn internetowych, która wciąż jest stosunkowo rzadka w projektowaniu witryn internetowych. Można ich również używać podczas porównywania witryn konkurencji w ramach analizy sytuacji. Podejście oparte na personie / scenariuszu klienta ma następujące zalety:

• Wspieranie zorientowania na klienta;

• Identyfikuje szczegółowe potrzeby informacyjne i kroki wymagane przez klientów;

• Może być używany zarówno do testowania istniejących projektów lub prototypów witryn internetowych, jak i do opracowywania nowych projektów;

• Może być używany do porównywania i testowania siły i jasności komunikacji propozycji na różnych stronach internetowych.

• Może być powiązany z określonymi wynikami marketingowymi wymaganymi przez właścicieli witryn.

Poniżej znajduje się kilka wskazówek i pomysłów na temat tego, co można uwzględnić podczas tworzenia postaci. Punktem początkowym lub końcowym jest nadanie każdej osobie imienia. Szczegółowe etapy to:

1 Zbuduj osobiste atrybuty w persony:

• Demograficzne: wiek, płeć, wykształcenie, zawód i B2B, wielkość firmy, pozycja w jednostce kupującej

• Psychograficzne: cele, zadania, motywacja

• Webografia: doświadczenie w sieci (miesiące), miejsce użytkowania (dom lub praca), platforma użytkowania (dial-up, szerokopasmowe), częstotliwość użytkowania, ulubione strony.

2 Pamiętaj, że persony to tylko modele cech i środowiska

• Cele projektowe

• Stereotypy

• Zwykle wystarczą trzy lub cztery, aby poprawić ogólną użyteczność, ale do określonych zachowań potrzeba więcej

• Wybierz jedną podstawową osobę, która jeśli jest zadowolona, oznacza, że inni będą prawdopodobnie zadowoleni.

3 Dla każdej osoby można opracować różne scenariusze, jak wyjaśniono poniżej. Napisz trzy lub cztery, na przykład:

• Scenariusz poszukiwania informacji (prowadzi do rejestracji witryny)

• Scenariusz zakupu - nowy klient (prowadzi do sprzedaży)

• Scenariusz zakupu - istniejący klient (prowadzi do sprzedaży).

Po opracowaniu różnych osobowości, które są reprezentatywne dla kluczowych typów odwiedzających witrynę lub typów klientów, czasami identyfikowana jest główna persona. Wodtke mówi: Twoja główna osobowość musi być zwykłym użytkownikiem, który jest zarówno ważny dla sukcesu biznesowego produktu, jak i potrzebujący z punktu widzenia projektowania - innymi słowy, początkujący użytkownik lub osoba z wyzwaniami technologicznymi. Mówi również, że można również rozwijać postacie drugorzędne, takie jak superużytkownicy lub zupełni nowicjusze. Osoby dopełniające się to takie, które nie mieszczą się w głównych kategoriach, które wykazują nietypowe zachowanie. Takie uzupełniające się postacie pomagają w myśleniu nieszablonowym ”i oferują wybory lub treści, które mogą być atrakcyjne dla wszystkich użytkowników. Aby zapoznać się z innym przykładem zastosowania person, zobacz mini studium przypadku dotyczące producenta farb Dulux, który wykorzystuje persony do projektowania swojej witryny i integracji z kampaniami medialnymi offline.

Aktorzy: ludzie, oprogramowanie lub inne urządzenia, które współpracują z systemem.

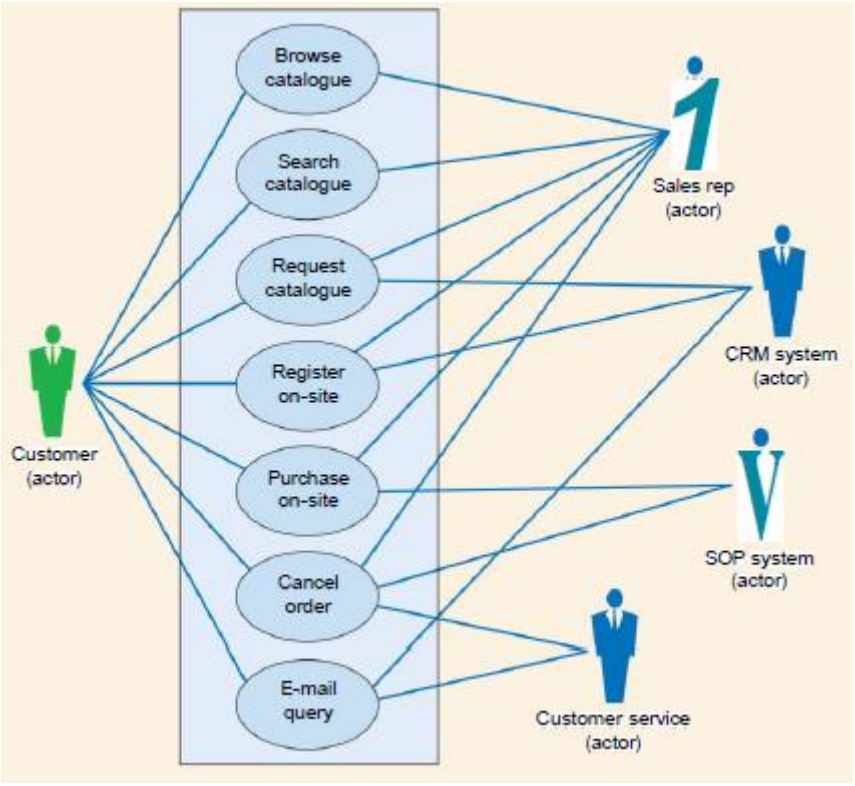
Etapy analizy przypadków użycia

Następujące etapy zostały zidentyfikowane przez Schneidera i Wintersa do analizy z wykorzystaniem metody przypadków użycia.

1 Zidentyfikuj aktorów

Aktorzy to te obiekty, które biorą udział w używaniu lub interakcji z systemem. Nie są częścią systemu. Oczywistymi aktorami są użytkownicy systemu. W aplikacji do obsługi klienta aktorami mogą być klient i osoba obsługująca klienta w firmie. Przeprowadzając analizę procesu w celu zdefiniowania przypadków użycia, zadajemy pytania takie jak: „Kim są aktorzy tego procesu?”, „Jakie usługi zapewniają ci aktorzy?”, „Jakie są zadania aktorów?” I „Jakie zmiany wprowadzają co do statusu całego procesu? ”. Aktorzy to zazwyczaj użytkownicy aplikacji, tacy jak klienci i pracodawcy. Mogą dodawać informacje do systemu lub otrzymywać je za pośrednictwem funkcji raportowania. Należy pamiętać, że pracownik pełniący kilka ról, takich jak rola kierownika i rola administratora, byłby reprezentowany przez dwóch różnych aktorów. Schneider i Winters (1998) zwracają uwagę, że inni aktorzy obejmują oprogramowanie i sprzętowe urządzenia sterujące, które zmieniają stan procesu, oraz zewnętrzne systemy, które współpracują z rozważanym systemem. Są to w rzeczywistości podmioty ludzkie, które zostały zautomatyzowane przez inne systemy, które współpracują z obecnym rozważanym systemem.

Aktorzy są oznaczani przy użyciu prostego podejścia pokazanego na rysunku



Przypadek użycia: sekwencja transakcji między aktorem a systemem, który wspiera działania aktora

Rozmowa: użytkownik ustnie opisuje wymagane działania.

Przewodnik: użytkownik wykonuje swoje działania za pomocą pliku system lub makieta.

Scenariusz: określona ścieżka lub przepływ zdarzeń lub działań w ramach przypadku użycia

2 Zidentyfikuj przypadki użycia

Przypadki użycia to różne rzeczy, które użytkownicy systemu chcą, aby wykonywał. Można je opisać jako czynności lub zadania, które są częścią dialogu między aktorem a systemem. Podsumowują wymagania systemu od każdego aktora, ponieważ opisują funkcjonalność, którą zapewni system. Typowe przypadki użycia to:

• Uruchamianie, zamykanie lub modyfikowanie systemu.

• Dodawanie lub zmienianie informacji w systemie. Przykłady obejmują złożenie zamówienia w handlu elektronicznym lub nagranie skargi za pośrednictwem poczty elektronicznej.

• Korzystanie z systemu raportowania lub wspomagania decyzji.

Niektóre przypadki użycia dla firmy B2C pokazano na rysunku powyższy. Bevan również zwraca uwagę na znaczenie zdefiniowania kluczowych scenariuszy użycia, co jest zgodne z opisanym powyżej podejściem do przypadków użycia. Ten etap, często nazywany „pozyskiwaniem wiedzy", obejmuje wywiady z użytkownikami i poproszenie ich o omówienie ich obecnego lub preferowanego sposobu pracy. Po ustaleniu scenariuszy można zastosować techniki sortowania kart, opisane przez Noyesa i Babera. Opisują, jak po przeprowadzeniu wywiadów z użytkownikami zapisywano na kartach typowe

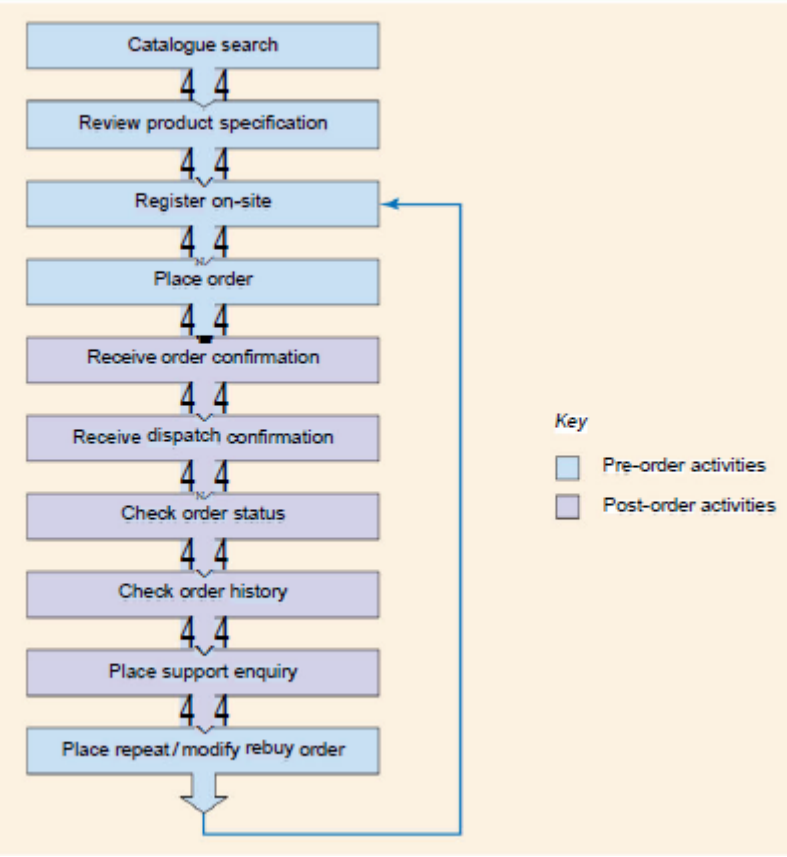
zadania lub czynności. Zostały one następnie wykorzystane do zidentyfikowania sekwencji działań wymaganych przez użytkowników w systemie menu. Wyjaśniają, że opracowany system menu był zupełnie inny niż ten przewidziany przez inżynierów oprogramowania. Techniki sortowania kart mogą być również wykorzystywane do sprawdzania, czy żadne z etapów nie zostało pominięte podczas przejścia - wykonywane jest przejście kart. Rozmowy nie wymagają fizycznej konfiguracji, ale przejścia w formie serii kart lub użycia prototypu systemu.

3 Powiązanie aktorów z przypadkami użycia

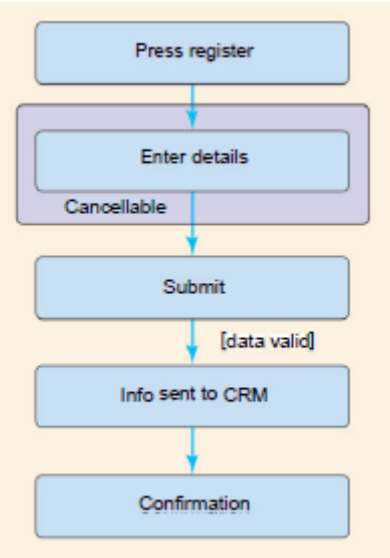
Rysunek powyższy pokazuje również, jak aktorzy odnoszą się do przypadków użycia. Może być używany do identyfikacji obowiązków i sprawdzania brakujących działań. Na przykład „Sprawdź stan zamówienia" to przypadek użycia, którego brakuje, a firma musiałaby omówić, czy akceptowalne jest, aby przedstawiciel obsługi klienta złożył zamówienie dla klienta, który narzekał na określony produkt.

4 Opracuj scenariusze przypadków użycia

Następnie opracowywany jest szczegółowy scenariusz w celu wyszczególnienia różnych ścieżek zdarzeń i działań dla każdego przypadku użycia. Scenariusz podstawowy opisuje typowy przypadek, w którym nic się nie dzieje. Przypadek użycia zawiera szczegóły działań lub funkcji, co się dzieje, gdy pojawia się alternatywa lub decyzja, lub gdy występuje błąd. Określono również warunki wstępne i warunki końcowe wyjścia z przypadku użycia. Rysunek przedstawia podstawowy scenariusz pełnego cyklu zakupów w handlu elektronicznym.



Bardziej szczegółowy scenariusz podstawowy dla „Rejestru" konkretnego przypadku użycia, napisany z punktu widzenia aktora-klienta z rysunku poniższego , przedstawia się następująco:



Warunek wstępny: użytkownik jest aktywny w witrynie internetowej.

Scenariusz: zarejestruj się.

Podstawowa ścieżka:

Przypadek użycia zaczyna się, gdy klient naciśnie „zarejestruj".

2 Klient podaje imię i nazwisko, adres pocztowy oraz e-mail.

3 Kod pocztowy / pocztowy i adres e-mail (symbol @) zostaną sprawdzone pod kątem ważności po wprowadzeniu, a użytkownik zapyta, czy wystąpił błąd.

4 Klient wybierze „prześlij".

5 System sprawdzi, czy wszystkie pola są obecne, a informacje o kliencie zostaną przekazane do systemu CRM.

6 Zostanie wyświetlona strona przekierowania, aby podziękować klientowi za rejestrację i umożliwić powrót do strony głównej, a przypadek użycia się kończy.

Stan końcowy: dane klienta zostały zapisane.

Alternatywne ścieżki: klient może anulować na etapach od 2 do 4 przed naciśnięciem przycisku „prześlij" i przypadkiem użycia kończy się

Można zauważyć, że określając w ten sposób przypadek użycia można wyjaśnić różne kwestie. Po ukończeniu scenariusza podstawowego można opracować scenariusze drugie lub alternatywne i dodać je do scenariuszy głównych jako alternatywne. W przypadku scenariusza rejestru anulowanie jest scenariuszem drugorzędnym; inne mogą zawierać warunki błędów, takie jak czy kod pocztowy jest nieprawidłowy. Architektura informacji: połączenie schematów organizacji, etykietowania i nawigacji, które tworzą system informacyjny

Projektowanie architektury informacji

Rosenfeld i Morville podkreślają znaczenie architektury informacji dla efektywnego projektowania witryn internetowych; mówią: Ważne jest, aby uznać, że każdy system informacyjny, czy to książka, czy intranet, ma architekturę informacyjną. 1 Dobrze opracowany "jest tutaj kluczem, ponieważ większość

witryn w ogóle nie ma zaplanowanej architektury informacji. Są analogiczne do budynków, które nie zostały wcześniej zaprojektowane. Decyzje projektowe odzwierciedlają osobiste uprzedzenia projektantów, przestrzeń nie zmienia się w czasie, technologie kierują projektem, a nie odwrotnie. W swojej książce Rosenfeld i Morville podają alternatywne definicje architektury informacji. Mówią, że jest:

1 Połączenie schematów organizacji, oznakowania i nawigacji w ramach systemu informacyjnego.

2 Projekt strukturalny przestrzeni informacyjnej ułatwiający realizację zadań i intuicyjny dostęp do treści.

3 Sztuka i nauka strukturyzowania i klasyfikowania witryn internetowych i intranetów w celu pomocy ludziom w znajdowaniu informacji i zarządzaniu nimi.

4 Nowa dyscyplina i społeczność praktyków skupiona na wprowadzaniu zasad projektowania i architektury do cyfrowego krajobrazu.

Mapa witryny: graficzne lub tekstowe przedstawienie relacji między różnymi grupami treści w witrynie internetowej.

Zasadniczo w praktyce tworzenie architektury informacji wiąże się z utworzeniem planu logicznego grupowania informacji - wiąże się to z utworzeniem struktury witryny, która jest często przedstawiana jako mapa witryny. Należy jednak pamiętać, że o architekturze informacji napisano całe książki, więc jest to z konieczności uproszczenie! Dobrze rozwinięta architektura informacji jest bardzo ważna dla użyteczności, ponieważ determinuje opcje nawigacji. Jest to również ważne dla optymalizacji wyszukiwarek (rozdział 9), ponieważ określa, w jaki sposób różne typy treści, których mogą szukać użytkownicy, są oznaczane i grupowane. Planowana architektura informacji jest niezbędna dla dużych witryn internetowych, takich jak transakcyjne witryny e-commerce, witryny właścicieli mediów i witryny służące do budowania relacji, które zawierają dużą ilość dokumentacji produktu lub pomocy technicznej. Architektury informacji są mniej ważne w przypadku małych witryn internetowych i witryn marek, ale nawet tutaj zasady można łatwo zastosować i mogą pomóc uczynić witrynę bardziej widoczną dla wyszukiwarek i użyteczną. Korzyści z tworzenia architektury informacji obejmują:

• Zdefiniowana struktura i kategoryzacja informacji będzie wspierać cele użytkownika i organizacji, tj. Jest to istotny aspekt użyteczności.

• Pomaga zwiększyć „przepływ" w witrynie - model myślowy użytkownika wskazujący, gdzie szukać treści, powinien odzwierciedlać treść witryny internetowej.

• Optymalizacja pod kątem wyszukiwarek - wyższe pozycje w rankingach wyszukiwania można często wykorzystać do uporządkowania i oznakowania informacji w uporządkowany sposób.

• Ma zastosowanie do integracji komunikacji offline - komunikacja offline, taka jak reklamy lub bezpośrednia poczta, może zawierać link do strony docelowej produktu lub kampanii, aby pomóc w uzyskaniu bezpośredniej reakcji, czasami nazywanej „odpowiedzią internetową". Może w tym pomóc rozsądna strategia adresów URL, opisana w rozdziale 8.

• Powiązane treści można pogrupować w celu zmierzenia skuteczności witryny internetowej w ramach projektowania do analizy, co również wyjaśniono poniżej.

Sortowanie kart lub klasyfikacja internetowa: proces porządkowania sposobu uporządkowania obiektów na stronie internetowej w sposób spójny.

Sortowanie kart

Korzystanie z sortowania kart to sposób, w jaki użytkownicy mogą aktywnie zaangażować się w proces rozwoju architektury informacji. Sortowanie kart jest przydatne, ponieważ witryny internetowe są często projektowane z perspektywy projektanta, a nie użytkownika informacji, co prowadzi do etykiet, grup tematycznych i kategorii, które nie są intuicyjne dla użytkownika. Sortowanie kart lub klasyfikacja internetowa powinny kategoryzować obiekty internetowe (np. Dokumenty) w celu ułatwienia realizacji zadań informacyjnych lub celów informacyjnych wyznaczonych przez użytkownika. Robertson wyjaśnia podejście do sortowania kart, które identyfikuje następujące pytania podczas korzystania z sortowania kart w celu ułatwienia procesu modelowania systemów klasyfikacji sieci:

• Czy użytkownicy chcą widzieć informacje pogrupowane według: tematu, zadania, grup biznesowych lub klientów lub rodzaju informacji?

• Jakie są najważniejsze pozycje do umieszczenia w menu głównym?

• Ile powinno być pozycji w menu i jak głęboko powinno być?

• Jak podobne lub różne są potrzeby użytkowników w całej organizacji?

Wybrane grupy użytkowników lub przedstawicieli otrzymają karty katalogowe, na których w zależności od celu sortowania kart zostanie zapisane:

• Rodzaje dokumentów

• Kluczowe słowa i pojęcia organizacyjne

• Tytuły dokumentów

• Opisy dokumentów

• Etykiety nawigacyjne.

Następnie grupy użytkowników mogą zostać poproszone o:

• Pogrupuj razem karty, które ich zdaniem odnoszą się do siebie;

• Wybierz karty, które dokładnie odzwierciedlają dany temat lub obszar;

• Organizuj karty pod względem hierarchii - terminy od wysokiego (szerokiego) do niskiego poziomu.

Pod koniec sesji analityk musi zabrać karty i zmapować wyniki w arkuszu kalkulacyjnym, aby znaleźć najpopularniejsze terminy, opisy i relacje. Jeżeli wykorzystywane są dwie lub więcej różnych grup, należy porównać wyniki i przeanalizować przyczyny różnic.

Plany: Pokaż relacje między stronami i innymi komponentami treści i mogą służyć do przedstawiania organizacji, nawigacji i systemów etykietowania.

Modele szkieletowe: znane również jako „schematy", sposób zilustrowania układu pojedynczej strony internetowej

Tworzenie scenorysów: Wykorzystanie statycznych rysunków lub zrzutów ekranu z różnych części witryny internetowej do przeglądu koncepcji projektu z użytkownikiem grupy. Można go wykorzystać do opracowania struktury - ogólnej „mapy" z poszczególnymi stronami pokazanymi osobno.

Plany

Według Rosenfelda i Morville'a schematy przedstawiają relacje między stronami a innymi składnikami treści i mogą służyć do przedstawiania systemów organizacji, nawigacji i etykietowania. Często są one

traktowane i określane jako mapy witryn lub diagramy struktury witryny i mają z nimi wiele wspólnego, z wyjątkiem tego, że są używane jako urządzenie projektowe, wyraźnie pokazujące grupy informacji i powiązania między stronami, a nie stronę w witryna internetowa wspomagająca nawigację.

Modele szkieletowe

Techniką pokrewną do planów są modele szkieletowe, które są używane przez projektantów stron internetowych do wskazania ostatecznego układu strony internetowej. Rysunek 11.15 pokazuje, że szkielet jest tak nazywany, ponieważ składa się tylko z konspektu strony z zawartością Vires, oddzielającą różne obszary treści lub nawigacji pokazane białymi znakami. Wodtke (2002) opisuje model szkieletowy (czasami nazywany „schematem") jako: podstawowy zarys pojedynczej strony, narysowany w celu wskazania elementów strony, ich relacji i ich względnego znaczenia. Dla wszystkich typów podobnych grup stron zostanie utworzony wireframe, zidentyfikowany na etapie planu (mapy serwisu) tworzenia architektury informacji.

Schematy ilustrują, w jaki sposób zawartość witryny internetowej jest powiązana i jak można się poruszać, podczas gdy szkielet koncentruje się na poszczególnych stronach; w przypadku modelu krawędziowego fokus nawigacji staje się miejscem, w którym zostanie umieszczony na stronie. Proces recenzowania modeli szkieletowych jest czasami określany jako „tworzenie scenariuszy", chociaż termin ten jest często używany do recenzowania kreatywnych pomysłów, a nie formalnej alternatywy projektowej. Wczesne projekty są rysowane na dużych kawałkach papieru lub makiety są tworzone przy użyciu programu do rysowania lub malowania. Na etapie wireframe nie kładzie się nacisku na użycie koloru lub grafiki, które zostaną opracowane we współpracy z zespołami brandingowymi lub marketingowymi oraz grafikami i zostaną zintegrowane z witryną pod koniec procesu tworzenia szkieletu.

Według Chaffey i Wooda celem modelu wireframe będzie:

• Zintegruj spójnie dostępne komponenty na stronie internetowej (np. Nawigacja, pola wyszukiwania);

• Porządkowanie i grupowanie kluczowych typów komponentów razem;

• Opracuj projekt, który skupi użytkownika na podstawowych wiadomościach i treściach;

• Prawidłowo wykorzystuj odstępy do strukturyzacji strony;

• Opracuj strukturę strony, która może być łatwo ponownie wykorzystana przez innych projektantów stron internetowych.

Szablon strony: standardowy format układu strony, który jest stosowany do każdej strony witryny internetowej. Zwykle definiowane dla różnych kategorii stron (np. Strona kategorii, strona produktu, strona wyszukiwania).

Kaskadowe arkusze stylów: Prosty mechanizm dodawania stylu (np. Czcionki, kolory, odstępy) do dokumentów internetowych. CSS umożliwia kontrolowanie różnych elementów stylu w całej witrynie lub jej sekcji. Elementy stylu, które są często kontrolowane, obejmują typografię, kolor tła i obrazy, obramowanie i marginesy.

Typowe funkcje szkieletu lub szablonu, które możesz napotkać, to:

• Nawigacja w kolumnach po lewej lub prawej stronie i na górze lub na dole.

• Obszary nagłówka i stopki.

• „Boksy” lub „portlety” - są to obszary treści, takie jak artykuł lub lista artykułów umieszczonych w ramkach na ekranie. Często boksy są dynamicznie wypełniane z systemu zarządzania treścią. Automaty na stronie głównej mogą służyć do:

• Podsumuj ofertę wartości online

• Pokaż promocje

• Polecaj powiązane produkty

• Nowości fabularne itp.

• zawierać reklamy.

Modele szkieletowe są następnie przekształcane w fizyczne szablony stron projektu witryny, które są obecnie tworzone przy użyciu standardowych kaskadowych arkuszy stylów (CSS), które umożliwiają wprowadzenie standardowego wyglądu i stylu w różnych sekcjach witryny. Menedżerom przydatne jest zrozumienie zasad CSS, ponieważ zapewnia to dużą elastyczność w podejmowaniu decyzji projektowych. Standard bodyW3C (www.w3.org) definiuje kaskadowe arkusze stylów (CSS) jako prosty mechanizm dodawania stylu (np. czcionki, kolory, odstępy) do dokumentów internetowych CSS umożliwia kontrolowanie różnych elementów stylu w całej witrynie lub jej sekcji. Elementy stylu, które są często kontrolowane, obejmują:

• Typografia

• Kolor tła i obrazy

• Granice i marginesy.

Arkusz stylów składa się z szeregu reguł, które kontrolują sposób wyświetlania wybranych elementów. Na przykład:

body {fon t - family: Verdana, Arial, Helvetica, SansSerif, Sans; font - size: 0.7em; text -align: center; margin: 0; background - color: white;

olor : black ; }

W tym przykładzie znacznik HTML „body” jest selektorem, a wymagany styl tekstu jest zdefiniowany między nawiasami klamrowymi to deklaracja.

Zalety CSS to:

• Przepustowość - strony są pobierane szybciej po pierwszym załadowaniu strony, ponieważ definicje stylów wystarczy pobrać raz jako osobny plik, a nie dla każdej strony;

• Bardziej efektywny rozwój - dzięki uzgodnieniu stylu serwisu i wdrożeniu w CSS jako części szablonów stron, projektowanie serwisu jest efektywniejsze;

• Skraca czas aktualizacji i konserwacji - znaczniki prezentacyjne są przechowywane w jednym miejscu, oddzielnie od treści, co przyspiesza globalną aktualizację witryny i zmniejsza ryzyko błędów;

• Zwiększona interoperacyjność - przestrzeganie zaleceń W3C pomaga w obsłudze wielu przeglądarek;

• Zwiększa dostępność - użytkownicy mogą łatwiej konfigurować wygląd lub dźwięki witryny za pomocą przeglądarek i innych narzędzi wspomagających dostępność. Witryna jest bardziej skłonna do

renderowania na różnych platformach dostępu, takich jak PDA i smartfony, i wydaje się być dobrze sformatowana na drukarkach

Orientacja na klienta: opracowywanie treści i usług witryny w celu przyciągnięcia uwagi różnych segmentów klientów lub innych odbiorców.

Orientacja na klienta

Dobrze zaprojektowana witryna zostanie stworzona, aby osiągnąć orientację na klienta lub koncentrację na klientach. Wiąże się to z trudnym zadaniem, jakim jest próba dostarczania treści i usług, które będą atrakcyjne dla szerokiego grona odbiorców. W przypadku firmy B2B trzy główne typy odbiorców to klienci, inne firmy i organizacje oraz pracownicy. Odwiedź witrynę internetową firmy Dell (www.dell.com), aby zobaczyć, jak firma Dell dzieli swoją bazę klientów na stronie głównej na:

• Małe biura i użytkownicy domowi

• Mały biznes

• Średnie firmy

• Duże firmy

• Korporacje

• Organizacje rządowe.

Pomyśl, jak dobrze działa to podejście. Jaka byłaby Twoja reakcja, gdybyś został sklasyfikowany jako zwykły właściciel małej firmy lub domu? Czy uważasz, że to prawidłowe podejście? Podobnym podejściem firmy Microsoft jest oferowanie specjalistycznej zawartości menedżerom IS, aby pomóc im w podejmowaniu decyzji inwestycyjnych. Czy właściwa jest bardziej prosta struktura zorientowana na produkty w witrynie internetowej? Oprócz segmentów klientów, projektanci muszą również wziąć pod uwagę różnice w pochodzeniu osób odwiedzających witrynę, które można traktować jako cztery różne rodzaje znajomości:

1 Znajomość internetu - czy osoby obeznane z Internetem mają na skróty? A czy jest pomoc dla nowicjuszy w prowadzeniu ich przez Twoją witrynę? Jak widzieliśmy w rozdziale 4, użytkownicy mają różny poziom znajomości sieci i należy to uwzględnić projekty witryn internetowych.

2 Znajomość organizacji - w przypadku klientów, którzy nie znają organizacji, potrzebna jest treść wyjaśniająca, kim jest firma, i wykazująca wiarygodność poprzez opcje „O nas” i opinie klientów.

3 Znajomość produktów organizacji - nawet obecni klienci mogą nie znać pełnej oferty produktów.

4 Znajomość witryny - mapy witryny, opcje wyszukiwania i pomocy to nie tylko „przyjemne” opcje dla witryny handlu elektronicznego, ponieważ możesz stracić potencjalnych klientów, jeśli nie można im pomóc, gdy zostaną zgubieni.

Jakob Nielsen tak mówi o początkujących użytkownikach:

Użytkownicy internetu są notorycznie kapryśni: wystarczy jedno spojrzenie na stronę główną i po kilku sekundach wychodzą, jeśli nie mogą tego rozgryźć. Duży wybór i łatwość poruszania się w innym miejscu kładą ogromny nacisk na to, że bardzo łatwo jest wejść na stronę. Ale zauważa, że musimy również wziąć pod uwagę ekspertów. Mówi, że w końcu możemy przejść do interfejsów, w których przeciętny odwiedzający witrynę otrzyma uproszczony projekt, który jest łatwy do nauczenia, a lojalni użytkownicy otrzymają zaawansowany projekt o większej mocy. Jednak na razie „szczegółowe treści i

zaawansowane informacje powinny być dodawane do witryn, aby zapewnić szczegółowość oczekiwaną przez ekspertów". Zasady orientacji na klienta można rozszerzyć z projektu witryny na taktyki stosowane do świadczenia usług za pośrednictwem witryny internetowej

Elementy projektu witryny

Po ustaleniu wymagań użytkownika możemy skierować naszą uwagę na projekt interfejsu człowiek-komputer. Nielsen dzieli swoją książkę na temat użyteczności sieciowej według trzech głównych obszarów, które można interpretować następująco:

1 Projekt i struktura serwisu - ogólna struktura serwisu.

2 Projekt strony - układ poszczególnych stron.

3 Projekt treści - w jaki sposób projektowany jest tekst i zawartość graficzna na każdej stronie.

Projekt i struktura witryny

Struktury tworzone przez projektantów dla witryn internetowych będą się znacznie różnić w zależności od ich odbiorców i celu witryny, ale możemy poczynić kilka ogólnych obserwacji na temat projektu i struktury. Przeanalizujemy czynniki, które projektanci biorą pod uwagę podczas projektowania stylu, organizacji i schematów nawigacji w witrynie.

Styl witryny

Efektywny projekt witryny internetowej będzie miał styl, który jest przekazywany za pomocą kolorów, obrazów, typografii i układu. Powinno to wspierać sposób pozycjonowania produktu lub jego markę.

Osobowość witryny

Elementy stylu można łączyć, aby stworzyć osobowość witryny. Możemy opisać osobowości witryny w taki sam sposób, w jaki opisujemy ludzi, na przykład „formalne" lub „zabawne". Taka osobowość musi być zgodna z potrzebami docelowej widowni. Odbiorcy biznesowi często potrzebują szczegółowych informacji i preferują styl obejmujący wiele informacji, taki jak w witrynie Cisco (www.cisco.com). Witryna konsumencka jest zwykle bardziej intensywna graficznie. Zanim projektanci przekażą swoje kreatywne projekty programistom, muszą również wziąć pod uwagę ograniczenia związane z wygodą użytkownika, takie jak rozdzielczość ekranu i głębia kolorów, używana przeglądarka i prędkość pobierania. Listę ograniczeń, które należy przetestować. Rosen i Purinton ocenili względne znaczenie czynników projektowych, które mają wpływ na konsumenta (na podstawie ankiet grupy uczniów).

Uważają, że istnieje kilka podstawowych czynników decydujących o skuteczności witryny e-commerce. Grupują te czynniki w następujący sposób:

(i) Spójność - prostota projektu, czytelność, wykorzystanie kategorii (do przeglądania produktów lub tematów), brak nadmiaru informacji, odpowiedni rozmiar czcionki, niezatłoczona prezentacja;

(ii) kategorie tekstu o różnej złożoności;

(iii) Czytelność - użycie „mini strony głównej" na każdej kolejnej stronie, to samo menu na każdej stronie, mapa serwisu.

Widać, że ci autorzy sugerują, że prostota w projektowaniu jest ważna. Inny przykład badań nad czynnikami projektowania witryn internetowych potwierdza znaczenie projektu.

Organizacja informacji: schematy Struktura wybrana do grupowania i kategoryzowania informacji.

Nawigacja w witrynie: schemat Narzędzia udostępnione użytkownikowi do poruszania się między nimi różne informacje w witrynie internetowej.

Przepływ: Przepływ opisuje, jak łatwo użytkownicy witryny mogą poruszać się między różnymi stronami z zawartością witryny.

Należy jednak pamiętać, że takie uogólnienia mogą wprowadzać w błąd w oparciu o zastosowaną metodologię. Zgłaszane zachowania (np. Poprzez kwestionariusze lub grupy fokusowe) mogą znacznie różnić się od rzeczywistych zachowań obserwowanych.

Organizacja witryny

W swojej książce na temat architektur informacji w sieci Rosenfeld i Morville identyfikują kilka różnych schematów organizacji informacji. Można je zastosować do różnych aspektów witryn e-commerce, od całej witryny po różne jej części. Rosenfeld i Morville określają następujące schematy organizacji informacji:

1 Dokładnie. Tutaj informacje mogą być naturalnie indeksowane. Jeśli weźmiemy przykład książek, mogą one być alfabetyczne - według autora lub tytułu; chronologicznie - według daty; lub w przypadku książek podróżniczych, na przykład geograficzne - według miejsca. Informacje w witrynie e-commerce mogą być prezentowane alfabetycznie, ale nie nadaje się do przeglądania.

2 Niejednoznaczne. Tutaj informacje wymagają klasyfikacji; ponownie biorąc przykład z książek, system dziesiętny Deweya jest niejednoznacznym schematem klasyfikacji, ponieważ bibliotekarze dzielą książki na dowolne kategorie. Takie podejście jest powszechne w witrynach handlu elektronicznego, ponieważ produkty i usługi można klasyfikować na różne sposoby. Inne niejednoznaczne schematy organizacji informacji, które są powszechnie stosowane na stronach internetowych, polegają na tym, że treść jest podzielona według tematu, zadania lub odbiorców. Użycie metafor jest również powszechne; metafora to sytuacja, w której witryna internetowa odpowiada znanej sytuacji w świecie rzeczywistym. Eksplorator Microsoft Windows, w którym informacje są pogrupowane według folderów, plików i kosza, jest przykładem metafory w świecie rzeczywistym. Stosowanie metafory koszyka zakupów jest szeroko rozpowszechnione w witrynach handlu elektronicznego. Należy jednak zauważyć, że Nielsen (2000b) uważa, że metafory mogą być mylące, jeśli metafora nie zostanie natychmiast zrozumiana lub zostanie źle zinterpretowana.

3 Hybrydowe. Tutaj będzie mieszanka schematów organizacyjnych, zarówno dokładnych, jak i niejednoznacznych. Rosenfeld i Morville (2002) zwracają uwagę, że stosowanie różnych podejść jest powszechne na stronach internetowych, ale może to prowadzić do nieporozumień, ponieważ użytkownik nie jest pewien, czym jest model mentalny aby być śledzonym. Można powiedzieć, że prawdopodobnie najlepiej jest zminimalizować liczbę schematów organizacji informacji.

Schematy nawigacji w witrynie

Opracowanie witryny, która jest łatwa w użyciu, zależy w dużej mierze od projektu schematu nawigacji w witrynie. Hoffman i Novak podkreślają znaczenie pojęcia „przepływu" w zarządzaniu użytecznością witryny. „Przepływ" zasadniczo opisuje, jak łatwo użytkownicy mogą znaleźć potrzebne informacje, przechodząc z jednej strony witryny do następnej, ale obejmuje również inne interakcje, takie jak wypełnianie formularzy na ekranie. Rettie podsumowuje znaczenie przepływu w kontekście online i podaje wskazówki, w jaki sposób można wykorzystać tę koncepcję do poprawy wrażeń odwiedzających. Pojęcie przepływu można lepiej zrozumieć, biorąc pod uwagę stwierdzenia opisujące przepływ, które pierwotnie były używane przez Csikszentmihalyi, a ostatnio przez badania Rettie w celu przetestowania przepływu na stronie internetowej:

(1) Mój umysł nie błąka się. Nie myślę o czymś innym. Jestem całkowicie zaangażowany w to, co robię. Moje ciało jest dobre. Wydaje się, że nic nie słyszę. Świat wydaje się być ode mnie odcięty. Jestem mniej świadoma siebie i swoich problemów.

(2) Moja koncentracja jest jak oddychanie. Nigdy o tym nie myślę. Po tym, jak naprawdę zaczynam, jestem naprawdę nieświadomy swojego otoczenia. Myślę, że mógłby zadzwonić telefon i dzwonek do drzwi, albo dom się spalił, czy coś w tym rodzaju. Kiedy zaczynam, naprawdę odgradzam się od całego świata. Kiedy przestanę, mogę znów to wpuścić.

(3) Jestem tak zaangażowany w to, co robię, że nie postrzegam siebie jako oddzielnego od tego, co robię.

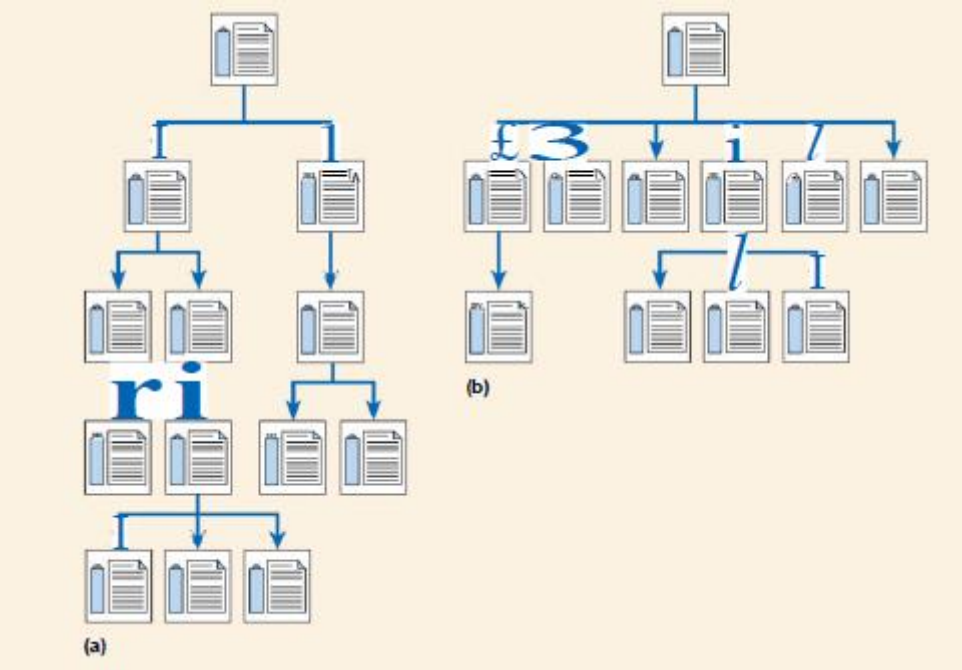
Rettie sugeruje, że następujące czynniki ograniczają przepływ: długie czasy pobierania, opóźnienia w pobieraniu wtyczek, długie formularze rejestracyjne, ograniczona stymulacja, nudne witryny, powolne odpowiedzi, witryny, które nie są intuicyjne, linki nawigacyjne, które zawodzą, wyzwanie większe niż umiejętności i nieistotna reklama. I odwrotnie, odwrócenie tych czynników może poprawić przepływ: szybkie czasy pobierania, wersje alternatywne (np. Tekst i grafika), automatyczne wypełnianie formularzy, możliwości interakcji, szybkie odpowiedzi, nawigacja, która tworzy wybory, przewidywalna nawigacja do kontroli, segmentacja według doświadczenia internetowego.

Wąska i głęboka nawigacja: mniej opcji, więcej kliknięć, aby dotrzeć do wymaganych treści.

Szeroka i płytka nawigacja: większy wybór, mniej kliknięć, aby dotrzeć do wymaganych treści.

Głębokie linki: termin Jakoba Nielsena określający użytkownika wchodzącego na stronę głęboko w jej strukturze.

Większość systemów nawigacji jest oparta na hierarchicznej strukturze serwisu. Podczas tworzenia konstrukcji projektanci muszą pójść na kompromis między dwoma podejściami przedstawionymi na rysunku



Zaletą takiego wąskiego i głębokiego podejścia jest mniej opcji wyboru na każdej stronie, co ułatwia użytkownikowi dokonanie wyboru, ale do uzyskania określonej informacji potrzeba więcej kliknięć. Szerokie i płytkie podejście wymaga mniejszej liczby kliknięć, aby dotrzeć do tego samego fragmentu informacji, ale projekt ekranu może zostać zagracony. Rysunek (a) przedstawia wąskie i głębokie podejście, a rysunek (b) szerokie i płytkie podejście. Należy zauważyć, że w takich przypadkach podejścia są odpowiednie odpowiednio dla odbiorców nietechnicznych i technicznych. Ogólna zasada jest taka, że projektanci witryn powinni upewnić się, że dostęp do dowolnej informacji w witrynie zajmuje tylko trzy kliknięcia. Oznacza to stosowanie szerokiego i płytkiego podejścia w większości dużych witryn. Może to być również korzystne dla celów SEO. Lynch i Horton zalecają szerokie i płytkie podejście i zauważają, że projektanci nie powinni wyobrażać sobie jednej strony głównej, na której klienci przychodzą do witryny, ale różnych stron głównych w zależności od różnych typów odbiorców. Nielsen zwraca uwagę, że wielu użytkowników nie trafia na stronę główną, ale mogą zostać przekierowani z innej witryny lub zgodnie z reklamą prasową lub telewizyjną do określonej strony, takiej jak www.b2b.com/jancomp. Nazywa ten proces „głębokim linkowaniem", a projektanci witryn powinni zapewnić odpowiednią nawigację i kontekst dla użytkowników przybywających na te strony. Oprócz kompromisów w zakresie głębokości linków w witrynie, konieczne jest również ograniczenie ilości miejsca przeznaczonego na menu. Nielsen zwraca uwagę, że niektóre witryny poświęcają tak dużo miejsca paskom nawigacyjnym, że przestrzeń dostępna dla treści jest ograniczona. Nielsen (2000c) sugeruje, że projektant systemów nawigacji powinien wziąć pod uwagę następujące informacje, które użytkownik witryny chce poznać:

• Gdzie ja jestem? Użytkownik musi wiedzieć, gdzie się znajduje w serwisie, co można wskazać poprzez zaznaczenie aktualnej lokalizacji i czytelne tytuły stron. Chaffey i inni określają to jako kontekst. Spójność lokalizacji menu na różnych stronach jest również wymagana, aby ułatwić rozpoznawanie. Użytkownicy muszą również wiedzieć, gdzie są w sieci. Wskazuje na to logo, które zgodnie z konwencją znajduje się w lewym górnym rogu strony.

• Gdzie ja byłem? Trudno jest to wskazać w witrynie, ale w przypadku czynności zorientowanych na zadania, takich jak zakup produktu, wyświetlacz może pokazać użytkownikowi, że znajduje się na n-tym etapie operacji, takiej jak dokonanie zakupu.

• Gdzie chcę iść? To jest główny system nawigacji, który daje opcje dla przyszłych operacji.

Aby odpowiedzieć na te pytania, wymagane jest jasne i zwięzłe oznakowanie. Preferowane są powszechnie stosowane standardy, takie jak Strona główna, Strona główna, Szukaj, Znajdź, Przeglądaj, Często zadawane pytania, Pomoc i O nas. Ale w przypadku innych konkretnych etykiet przydatne jest posiadanie tego, co Rosenfeld i Morville nazywają „uwagami dotyczącymi zakresu" - dodatkowym wyjaśnieniem. Autorzy ci również sprzeciwiają się używaniu ikonicznych etykiet lub obrazów bez odpowiedniego tekstu, ponieważ są one podatne na błędną interpretację i ich przetwarzanie zajmuje więcej czasu. Ponieważ korzystanie z systemu nawigacji może nie umożliwić użytkownikowi szybkiego znalezienia potrzebnych informacji, projektanci witryny muszą zapewnić alternatywne rozwiązania. Te alternatywy obejmują funkcje wyszukiwania, wyszukiwania zaawansowanego, przeglądania i mapy witryny. Whatis.com (www.whatis.com) dobrze ilustruje te funkcje.

Projekt strony

Projekt strony polega na stworzeniu odpowiedniego układu dla każdej strony. Główne elementy układu strony to tytuł, nawigacja i treść. Standardową zawartość, taką jak prawa autorskie, można dodać do każdej strony jako stopkę. Problemy z projektem strony obejmują:

• Elementy strony. Odsetek strony poświęconej treści w porównaniu do wszystkich innych treści, takich jak nagłówki, stopki i elementy nawigacyjne. Należy również wziąć pod uwagę lokalizację tych elementów. Menu główne zwykle znajduje się na górze lub po lewej stronie. Zastosowanie systemu menu u góry okna przeglądarki zapewnia więcej miejsca na zawartość poniżej.

• Stosowanie ramek. Jest to generalnie odradzane z powodów podanych w Części 12.

• Zmiana rozmiaru. Dobry projekt układu strony powinien umożliwiać użytkownikowi zmianę rozmiaru tekstu lub pracę z różnymi rozdzielczościami monitora.

• Konsystencja. Układ strony powinien być podobny we wszystkich obszarach serwisu, chyba że potrzeba więcej miejsca, na przykład na forum dyskusyjne lub prezentację produktu. Standardy koloru i typografii można egzekwować za pomocą kaskadowych arkuszy stylów.

• Drukowanie. Układ powinien umożliwiać drukowanie lub zapewniać alternatywny format druku.

Projektowanie treści

Copywriting w Internecie to ewoluująca forma sztuki, ale wiele zasad dobrego copywritingu jest takich samych, jak dla każdego medium. Typowe błędy, które widzimy na stronach internetowych to:

• zbyt duża wiedza przyjęta od gościa o firmie, jej produktach i usługach;

• używanie wewnętrznego żargonu dotyczącego produktów, usług lub działów - używanie nierozpoznawalnych akronimów.

Copywriterzy internetowi muszą również wziąć pod uwagę użytkownika czytającego treść na ekranie. Podejścia do radzenia sobie z ograniczeniami narzuconymi przez klienta przy użyciu monitora obejmują:

• pisanie bardziej zwięźle niż w broszurach;

• dzielenie lub dzielenie tekstu na maksymalnie 5-6 wierszy; pozwala to użytkownikom raczej skanować niż czytać informacje na stronach internetowych;

• używanie list z nagłówkami pisanymi większą czcionką;

• nigdy nie umieszczaj zbyt wiele na jednej stronie, z wyjątkiem przedstawiania obszernych informacji, takich jak raport, który może być łatwiejszy do odczytania na jednej stronie;

• używanie hiperłączy w celu zmniejszenia rozmiarów stron lub ułatwienia przepływu w ramach kopii, poprzez tworzenie linków do sekcji znajdujących się w dalszej części strony lub łączenie do innej strony.

Hofacker opisuje pięć etapów przetwarzania informacji przez człowieka podczas korzystania z witryny internetowej. Można je zastosować zarówno do projektowania stron, jak i do projektowania treści, aby poprawić użyteczność i pomóc firmom w dotarciu do konsumentów. Każdy z pięciu etapów stanowi przeszkodę, ponieważ jeśli projekt witryny lub treść są zbyt trudne do przetworzenia, klient nie może przejść do następnego etapu. Warto rozważyć poszczególne etapy, aby zminimalizować trudności. Korzystając z tych warstw, możemy mapować zawartość na różnych poziomach dostępu, aby stworzyć witrynę, która jest zintegrowana z potrzebami jej odbiorców. Dotyczy to również sekcji dotyczącej bezpieczeństwa, ponieważ różne poziomy dostępu mogą być przypisane do różnych informacji

Dostępność: Podejście do projektowania witryny mające na celu dostosowanie korzystania z witryny przy użyciu różnych przeglądarek i ustawień, szczególnie wymaganych przez osoby niedowidzące

GPRS: General Packet Radio Services to standard oferujący mobilny transfer danych i dostęp do WAP około 5 do 10 razy szybciej niż tradycyjny dostęp GSM.

Dostępność sieci

Dostępność sieci to kolejny podstawowy wymóg dotyczący witryn internetowych. Chodzi o umożliwienie wszystkim użytkownikom witryny internetowej interakcji z nią, niezależnie od ich niepełnosprawności lub przeglądarki internetowej lub platformy, z której korzystają, aby uzyskać dostęp do witryny. Osoby niedowidzące są głównymi odbiorcami, którym może pomóc zaprojektowanie dostępnej witryny internetowej. Jednak zwiększone wykorzystanie mobilnych lub bezprzewodowych urządzeń dostępowych, takich jak osobiste asystenty cyfrowe (PDA) i telefony GPRS lub 3G, również powoduje, że kwestia dostępności jest ważna. Poniższy cytat pokazuje, jak ważna jest dostępność witryny internetowej dla niedowidzącego użytkownika, który używa czytnika ekranu, który odczytuje opcje nawigacji i zawartość witryny internetowej. Dla mnie bycie online jest wszystkim. To moje Hi-Fi, to moje źródło powitania, to mój supermarket, to mój telefon. To moja droga. (Lynn Holdsworth, użytkownik czytnika ekranu, twórca stron internetowych i programista, RNIB, www.rnib.org.uk)

Prawodawstwo dotyczące dostępności: prawodawstwo mające na celu ochronę niepełnosprawnych użytkowników witryn internetowych, w tym osób z niepełnosprawnością wzroku

Pamiętaj, że w wielu krajach obowiązują obecnie szczególne przepisy dotyczące dostępności, którym podlegają właściciele witryn internetowych. Jest to często zawarte w aktach dotyczących niepełnosprawności i dyskryminacji. W Wielkiej Brytanii stosowną ustawą jest Ustawa o niepełnosprawności i dyskryminacji (DDA) z 1995 r. Niedawne zmiany w DDA wprowadzają niezgodną z prawem dyskryminację osób niepełnosprawnych w sposobie, w jaki firma rekrutuje i zatrudnia ludzi, świadczy usługi lub zapewnia edukację. Świadczenie usług jest częścią prawa mającą zastosowanie do projektowania witryn internetowych. Udostępnianie witryn internetowych jest wymogiem części II ustawy o niepełnosprawności i dyskryminacji opublikowanej w 1999 r. I wymaganym przez prawo z 2002 r. Kodeks postępowania z 2002 r. Zawiera wymóg prawny dotyczący dostępności witryn internetowych. Jest to najważniejsze w przypadku witryn, które oferują usługi; na przykład kodeks postępowania podaje następujący przykład: Przedsiębiorstwo lotnicze udostępnia publicznie usługę rezerwacji i rezerwacji lotów na swojej stronie internetowej. Jest to świadczenie usługi i podlega ustawie. Chociaż istnieje moralny imperatyw dostępności, istnieje również imperatyw biznesowy, aby zachęcić firmy do zapewnienia dostępności swoich witryn internetowych. Główne argumenty przemawiające za dostępnością to:

1 Liczba osób niedowidzących - w wielu krajach są miliony osób niedowidzących, od „daltonistów” do niedowidzących do niewidomych.

2 Liczba użytkowników mniej popularnych przeglądarek lub różnica w rozdzielczości ekranu. Microsoft Internet Explorer jest obecnie dominującą przeglądarką, ale są mniej znane przeglądarki, które mają lojalnych fanów wśród niedowidzących (na przykład czytniki ekranu i Lynx, przeglądarka tekstowa) i wczesnych użytkowników (na przykład Mozilla Firefox, Safari i Opera). Jeśli witryna internetowa nie wyświetla się dobrze w tych przeglądarkach, możesz stracić tych odbiorców.

3 Więcej odwiedzających z naturalnych list wyszukiwarek. Wiele technik zwiększania użyteczności witryn pomaga również w optymalizacji pod kątem wyszukiwarek. Na przykład jaśniejsza nawigacja, alternatywne tekstowe obrazy i mapy witryn mogą pomóc poprawić pozycję witryny w rankingach wyszukiwarek.

4 Wymogi prawne. W wielu krajach udostępnianie witryn internetowych jest prawnie wymagane. Na przykład w Wielkiej Brytanii obowiązuje ustawa o dyskryminacji osób niepełnosprawnych, która tego wymaga. Wymagania tych praw opisano bardziej szczegółowo w dalszej części tego tematu.

Wytyczne dotyczące tworzenia dostępnych witryn internetowych są opracowywane przez rządy różnych krajów i organizacje pozarządowe, takie jak organizacje charytatywne. Organizacje zajmujące się normami internetowymi takie jak World Wide Web Consortium były aktywne w promowaniu wytycznych dotyczących dostępności sieci poprzez Inicjatywę Dostępności Stron Internetowych (WAI), patrz www.w3.org/WAI. Opisuje typowe problemy z dostępnością, takie jak: obrazy bez tekstu alternatywnego; brak tekstu alternatywnego dla hot-spotów mapy obrazowej; wprowadzające w błąd użycie elementów strukturalnych na stronach; nieopisany dźwięk lub nieopisane wideo; brak alternatywnych informacji dla użytkowników, którzy nie mają dostępu do ramek lub skryptów; tabele, które są trudne do rozszyfrowania podczas linearyzacji; lub witryny o słabym kontraście kolorów. Pełniejsza lista kontrolna dotycząca zgodności dostępności przy projektowaniu witryn internetowych i kodowaniu za pomocą HTML jest dostępna w World Wide Web Consortium (www.w3.org/TR/WCAG10/full-checklist.html). Istnieją trzy różne poziomy priorytetów, które opisuje w następujący sposób:

• Priorytet 1 (Poziom A). Twórca treści WWW musi spełnić ten punkt kontrolny. W przeciwnym razie co najmniej jedna grupa nie będzie mogła uzyskać dostępu do informacji w dokumencie. Spełnienie tego punktu kontrolnego jest podstawowym wymogiem dla niektórych grup, aby móc korzystać z dokumentów internetowych.

• Priorytet 2 (Poziom AA). Twórca treści WWW powinien spełnić ten punkt kontrolny. W przeciwnym razie co najmniej jedna grupa będzie miała trudności z dostępem do informacji w dokumencie. Spełnienie tego punktu kontrolnego usunie istotne bariery w dostępie do dokumentów internetowych.

• Priorytet 3 (poziom AAA). Twórca treści internetowych może zająć się tym punktem kontrolnym. W przeciwnym razie co najmniej jedna grupa będzie miała nieco trudności z dostępem do informacji w dokumencie. Spełnienie tego punktu kontrolnego poprawi dostęp do dokumentów internetowych. Tak więc dla wielu firm standardem jest spełnienie Priorytetu 1 i Priorytetu 2 lub 3, jeśli jest to praktyczne. Niektóre z najważniejszych elementów Priorytetu 1 są opisane w tych „Krótkich wskazówkach" WAI:

• Obrazy i animacje. Użyj tagów alt, aby opisać funkcję każdej wizualizacji.

• Mapy obrazu. Użyj mapy i tekstu po stronie klienta dla punktów aktywnych.

• Multimedia. Zapewnij podpisy i transkrypcje nagrania audio oraz opisy wideo.

• Linki hipertekstowe. Używaj tekstu, który ma sens, gdy jest czytany poza kontekstem. Na przykład unikaj „kliknij tutaj".

• Organizacja strony. Używaj nagłówków, list i spójnej struktury. Tam, gdzie to możliwe, używaj CSS do układu i stylu.

• Wykresy i wykresy. Podsumuj lub użyj atrybutu longdesc

• Skrypty, aplety i wtyczki. Zapewnij alternatywną zawartość na wypadek, gdyby aktywne funkcje były niedostępne lub nieobsługiwane.

• Ramy. Użyj elementu noframes i znaczących tytułów.

• Tabele. Uczyń sensowne czytanie wiersz po wierszu. Podsumować.

• Sprawdź swoją pracę. Uprawomocnić. Skorzystaj z narzędzi, listy kontrolnej i wytycznych dostępnych na stronie www.w3.org/TRAA/CAG

Tagi Alt: tagi Alt pojawiają się po tagu obrazu i zawierają

fraza związana z tym obrazem. Na przykład:

<img src = „logo.gif”

alt = „Nazwa firmy,

produkty firmy ”/>

Bezpieczeństwo projektu dla e-biznesu

Bezpieczeństwo jest głównym problemem menedżerów e-biznesu. Głównym problemem jest bezpieczeństwo informacji: zarówno o klientach, jak i wewnętrznych danych firmowych dotyczących finansów, logistyki, marketingu i pracowników. Rzeczywiście, widzieliśmy w rozdziale 4, że zabezpieczenie informacji o klientach jest wymogiem prawnym wynikającym z przepisów o ochronie danych w wielu krajach. Ryzyko to dotyczy wszystkich firm, dużych i małych. Większe firmy są zwykle bardziej narażone na ataki ukierunkowane, których celem jest zakłócanie usług. Informacje wykorzystywane w systemach e-biznesu muszą być chronione przed szeregiem zagrożeń.

CAPTCHA: Captcha oznacza „‘Completely Automated Public Turing test to tell Computers and Humans Apart’”. Wymaga to od osoby przesłania formularza internetowego, takiego jak komentarz, aby wprowadzić litery lub numery z obrazu, aby potwierdzić, że są prawdziwymi użytkownikami.

Złośliwe oprogramowanie: złośliwe oprogramowanie lub paski narzędzi, zwykle pobierane za pośrednictwem Internetu, który działa jak koń trojański, wykonując inne niepożądane czynności, takie jak rejestrowanie kluczy haseł użytkowników lub wirusy, które mogą zbierać adresy e-mail

Phishing: uzyskiwanie danych osobowych online za pośrednictwem witryn i e-maili podszywających się pod legalne firmy.

Firewall: Specjalistyczna aplikacja instalowana na serwerze w miejscu, w którym firma jest podłączona do Internetu. Jego celem jest zapobieganie nieautoryzowanemu dostępowi do firmy z zewnątrz.

Atak typu „odmowa usługi”: znany również jako rozproszony atak typu „odmowa usługi” (DDOS), polega na przejęciu kontroli przez grupę hakerów nad wieloma komputerami „zombie” podłączonymi do Internetu, których bezpieczeństwo zostało ograniczone. Ten „botnet” jest następnie używany do wysyłania wielu żądań do serwera docelowego, co powoduje jego przeciążenie i uniemożliwia dostęp innym odwiedzającym.

System zarządzania bezpieczeństwem informacji: proces organizacyjny do ochrony zasobów informacyjnych.

Polityka bezpieczeństwa informacji: definicja podejścia organizacji do bezpieczeństwa informacji i obowiązki pracowników w zakresie ochrony informacji.

Rejestr zasobów informacyjnych (IAR): repozytorium typów, wartości i własności wszystkich informacji w organizacji.

Zarządzanie ciągłością biznesową lub odtwarzanie po awarii: środki podjęte w celu zapewnienia możliwości przywrócenia informacji i dostępu do nich w przypadku zniszczenia pierwotnych informacji i metody dostępu.

Biorąc pod uwagę zakres zagrożeń bezpieczeństwa ,wiele organizacji wdraża obecnie formalny system zarządzania bezpieczeństwem informacji. Strategia zarządzania informacjami będzie wymagała wprowadzenia polityki bezpieczeństwa informacji. Może to być polityka opracowana wewnętrznie lub przyjęcie standardu bezpieczeństwa, takiego jak Brytyjska norma BS 7799, która została zaktualizowana i ratyfikowana jako norma międzynarodowa ISO / IEC 17799. Oparłem opis w tym wydaniu zarządzania e-biznesem i handlem elektronicznym na ISO 17799, ponieważ obejmuje on kompleksowe omówienie różnych zagrożeń i podejść do zarządzanie bezpieczeństwem. Zaleca następujące procesy:

1 Plan - przeprowadź analizę ryzyka biznesowego

2 Kontrole wewnętrzne w celu zarządzania odpowiednim ryzykiem

3 Sprawdź - przegląd kierownictwa w celu weryfikacji skuteczności

4 Działania - zmiany działań wymagane w ramach przeglądu, jeśli to konieczne.

ISO 17799 / BS 7799 zapewnia międzynarodową normę, która pomaga stworzyć ramy zarządzania ryzykiem .Wymaga zdefiniowania następujących obszarów zarządzania bezpieczeństwem informacji:

• Sekcja 1: Polityka bezpieczeństwa. Opisuje wymagania organizacji i zakres zabezpieczeń dla różnych obszarów biznesowych i witryn. Powinien również wykazywać wsparcie wyższego kierownictwa w kontrolowaniu i posiadaniu zabezpieczeń.

• Część 2: Bezpieczeństwo organizacji. Opisuje, w jaki sposób firma zarządza bezpieczeństwem, w tym różne obowiązki personelu związane z bezpieczeństwem, w jaki sposób incydenty bezpieczeństwa są zgłaszane, podejmowane i przeglądane jako standardowa działalność biznesowa w celu poprawy bezpieczeństwa.

• Sekcja 3: Klasyfikacja i kontrola zasobów. Jest to podobne do sporządzania inwentaryzacji aktywów fizycznych, takich jak komputery, drukarki, maszyny, pojazdy itp. Wymaga to audytu informacji z pytaniami takimi jak „Ile kosztuje uzyskanie? Ile kosztowałaby wymiana? Jaki jest zakres szkody wyrządzonej organizacji, gdyby została ujawniona opinii publicznej lub konkurentowi? ". Odpowiadając na te pytania i opracowując spis różnych typów zasobów informacyjnych, można wprowadzić odpowiednie zabezpieczenia. BS 7799 zaleca utworzenie rejestru zasobów informacyjnych (IAR), wyszczególniającego wszystkie zasoby informacyjne w organizacji, takie jak bazy danych, rejestry personelu, umowy, licencje na oprogramowanie, materiały reklamowe. Dla każdego zasobu zdefiniowano odpowiedzialność. Następnie można określić wartość każdego składnika aktywów, aby zapewnić odpowiednie zabezpieczenie.

• Sekcja 4: Bezpieczeństwo personelu. Zapewnia to przejrzystość definicji stanowisk i umów o pracę, zmniejsza ryzyko błędu ludzkiego prowadzącego do utraty informacji oraz zapewnia, że pracownicy rozumieją swoje prawa i obowiązki w zakresie bezpieczeństwa informacji. Aby to osiągnąć, ważne jest również szkolenie personelu. Przykład materiału edukacyjnego, który jest publicznie dostępny dla Massachusetts Institute of Technology: http://web.mit.edu/ist/topics/security/.

• Część 5: Bezpieczeństwo fizyczne i środowiskowe. Określa fizyczny dostęp do budynków. Rozważa również, w jaki sposób można chronić informacje przed zagrożeniami, takimi jak pożar i powódź.

• Część 6: Komunikacja i zarządzanie operacyjne. Wytyczne dotyczące codziennej obsługi systemów informatycznych to największa sekcja normy BS 7799. Obejmuje ona kryteria akceptacji dla nowych lub zaktualizowanych systemów, oprogramowania do ochrony przed wirusami, korzystania z poczty e-

mail i witryn internetowych, dostępu do sieci oraz systemów tworzenia kopii zapasowych i przywracania. .

• Część 7: Kontrola dostępu. Definiuje, jak chronić dostęp do systemów informatycznych poprzez mechanizmy kontroli dostępu (procedury związane z nazwą użytkownika i hasłem z różnymi poświadczeniami bezpieczeństwa dla różnych aplikacji i typów informacji).

• Część 8: Rozwój i konserwacja systemu. Określa, w jaki sposób nowe systemy muszą być projektowane i zamawiane z uwzględnieniem bezpieczeństwa.

• Część 9: Zarządzanie ciągłością działania. Zarządzanie ciągłością biznesową lub odtwarzanie po awarii określa, w jaki sposób organizacja będzie mogła nadal funkcjonować w przypadku poważnego zdarzenia, takiego jak pożar, powódź lub inne uszkodzenia systemów informatycznych. Kluczem do tego jest korzystanie z zewnętrznych kopii zapasowych i systemów alternatywnych.

• Część 10: Zgodność. Określa, w jaki sposób organizacja będzie przestrzegać odpowiednich przepisów Wielkiej Brytanii i UE związanych z zarządzaniem bezpieczeństwem informacji, w tym przepisów BHP - ustawy o ochronie danych, ustawy o nadużyciach komputerów, ustawy o wzorach, prawach autorskich i patentach, ustawy o prawach człowieka. Wdrożenie BS 7799 to dobry sposób na zapewnienie, że firma spełnia te wymagania. Aby zapewnić zgodność organizacji, należy przeprowadzać regularne audyty i przeglądy.

Omówimy teraz niektóre z głównych zagrożeń bezpieczeństwa w e-biznesie, którymi należy zarządzać.

Wirus komputerowy: program zdolny do samoreplikacji, który na to pozwala na przenoszenie z jednej maszyny na drugą. Może być złośliwy i usunąć dane lub łagodny.

Wirus sektora rozruchowego: zajmuje rekord rozruchowy dysków twardych i dyskietek i jest aktywowany podczas uruchamiania komputera.

Robak: mały program, który sam się powiela i przenosi w sieci z jednego komputera na drugi. Forma wirusa

Trojan: wirus podszywający się pod uczciwą aplikację.

Zarządzanie wirusami komputerowymi

Wirusy komputerowe stanowią poważne zagrożenie dla firm i danych osobowych, ponieważ szacuje się, że jest ich obecnie ponad 100 000.

Rodzaje wirusów

Istnieje wiele różnych mechanizmów, za pomocą których wirusy komputerowe przenoszą się z jednej maszyny na drugą. Wszystkie wykorzystują jakąś technikę, aby wirus rozmnażał się lub „samoreplikował", a następnie przenosił na inny komputer. Omówimy teraz pokrótce główne typy wirusów komputerowych, przed którymi muszą się chronić firmy.

1 Wirus sektora startowego. Wirusy sektora startowego były najważniejsze, gdy dyskietki były powszechnie używane.

2 Robak to mały program komputerowy, który replikuje się, a następnie przenosi z jednej maszyny na drugą. Ponieważ nie jest wymagana interakcja człowieka, robaki mogą się rozprzestrzeniać bardzo szybko. Na przykład robak „Code Red" replikował się ponad 250 000 razy w ciągu zaledwie 9 godzin w dniu 19 lipca 2001 r. W 2003 r. Robak „Slammer" wykorzystał lukę w zabezpieczeniach w produkcie bazodanowym Microsoft SQL Server i szybko zainfekował 75 000 maszyn. Każda zainfekowana

maszyna wysyłała tak duży ruch, że wiele innych serwerów również uległo awarii. Jak pokazano na rysunku 11.20, był to jeden z najszybciej rozprzestrzeniających się wirusów wszechczasów. Wygląda na to, że w przyszłości takie robaki spowodują całkowity zastój w Internecie.

3 Makrowirusy. Makrowirusy są doczepiane do dokumentów utworzonych przez aplikacje biurowe, takie jak Microsoft Word i Excel. Oprogramowanie biurowe, takie jak to, ma funkcję makr, która pomaga użytkownikom rejestrować typowe czynności, takie jak formatowanie, lub tworzyć bardziej złożone aplikacje w języku Visual Basic for Applications (VBA). Jednym z najbardziej znanych makrowirusów jest „Melissa". Nastąpiło to w marcu 1999 r. i wyznaczyło nowy trend, ponieważ połączyło makrowirusa z wirusem, który uzyskiwał dostęp do książki adresowej programu Microsoft Outlook w celu wysyłania wiadomości e-mail do nowych ofiar. Był to jeden z najszybciej rozprzestrzeniających się wirusów w historii i szacuje się, że wpłynął na ponad milion komputerów. W 2002 r. autor wirusa „Melissa", David L. Smith, został skazany na 20 miesięcy więzienia w USA.

4 Wirusy załączników e-mail. Wirusy te są aktywowane, gdy użytkownik programu pocztowego otwiera załącznik. „Przykładem takiego wirusa jest Melissa. Wirus „Love Bug" zawiera temat „Kocham cię", podczas gdy wiadomość zawiera tekst „proszę sprawdź załączony LOVELETTER ode mnie", który jest załączonym plikiem o nazwie LOVE-LETTER-FORYOU. TXT.VBS. Wirus usunął pliki graficzne i dźwiękowe oraz uzyskał dostęp do serwerów internetowych, aby wysłać różne wersje samego siebie. Według ClickZ (2003) oszacowano, że ten wirus wyrządził prawie 9 miliardów dolarów szkód. Większość kosztów to nie utrata danych, ale koszt zatrudnienia specjalistów w celu rozwiązania problemu lub stracony czas personelu.

5 Wirusy trojańskie. Trojan to wirus podszywający się pod uczciwą aplikację. Ich nazwa pochodzi od greckiego mitu o olbrzymim drewnianym koniu używanym przez napastników do uzyskania dostępu do Troi w celu zaatakowania go. Przykłady obejmują narzędzia, takie jak program do udostępniania plików, wygaszacz ekranu, aktualizacje niektórych składników systemu, a nawet imitacje programów antywirusowych. Zaletą twórców wirusów jest to, że programy mogą być znacznie większe. Jednym z najbardziej znanych trojanów jest „Back Orifice", rzekomo opracowany przez grupę hakerską znaną jako „Cult of the Dead Cow". Można to było dołączyć do innych większych plików i dać hakerowi pełny dostęp do maszyny.

6 Wirusy fałszywe wiadomości e-mail. Są to ostrzeżenia o wirusach, które nie są prawdziwymi wirusami, które proszą odbiorcę o wysłanie ostrzeżenia do swoich znajomych. Zwykle są złośliwe, ale mogą zawierać instrukcje dotyczące usuwania wirusa poprzez usuwanie plików, które mogą spowodować uszkodzenia. Powodują zakłócenia w utraconym czasie.

Oprogramowanie antywirusowe: oprogramowanie do wykrywania i eliminowania wirusów.

Zarządzana usługa e-mail: odbiór i przesyłanie e-maili jest zarządzane przez stronę trzecią.

Ochrona systemów komputerowych przed wirusami

Wszystkie organizacje i osoby wymagają polityki zwalczania potencjalnego wpływu wirusów, biorąc pod uwagę częstotliwość, z jaką są uwalniane nowe, szkodliwe wirusy. Nawet indywidualni użytkownicy komputerów w domu powinni przemyśleć kroki, jakie mogą podjąć, aby przeciwdziałać wirusom. Istnieją dwa podejścia, które można połączyć w celu zwalczania wirusów. Korzystają z odpowiednich narzędzi i edukują personel, aby zmieniać praktyki. Oprogramowanie antywirusowe jest dobrze znane jako narzędzie do ochrony systemów przed wirusami. Wiele firm i domów korzysta obecnie z produktów, takich jak McAfee Virus Scan i Symantec Norton Anti-Virus, w celu ochrony przed wirusami. Niestety, aby oprogramowanie antywirusowe było skuteczne, potrzeba znacznie więcej

działań niż początkowy zakup. Widzieliśmy powyżej, że stale pojawiają się nowe wirusy. Dlatego ważne jest, aby uzyskiwać regularne aktualizacje, a to często się nie zdarza, ponieważ musi istnieć proces wyzwalający aktualizacje, takie jak comiesięczna aktualizacja. Firmy muszą również zdecydować o częstotliwości skanowania pamięci i plików komputerowych, ponieważ pełne skanowanie przy uruchomieniu może zająć dużo czasu. Większość programów antywirusowych stara się teraz zidentyfikować wirusy, gdy pojawiają się one po raz pierwszy (skanowanie w czasie rzeczywistym). Kolejną kwestią jest to, jak dobrze narzędzie antywirusowe identyfikuje wiadomości e-mail i makrowirusy, ponieważ identyfikacja tego typu wirusów jest trudniejsza. Innym podejściem do zwalczania wirusów pocztowych jest użycie zewnętrznej zarządzanej usługi poczty e-mail, która skanuje wiadomości e-mail przed ich przybyciem do organizacji, a następnie skanuje wiadomości e-mail w poszukiwaniu wirusów, gdy są wysyłane. Na przykład Messagelabs (www.messagelabs.com) skanuje dziennie 2,7 miliarda wiadomości e-mail dla 7500 firm na całym świecie. W sierpniu 2008 roku poinformował, że:

• 78% wiadomości to spam

• 1 na 88 zawierał wirusa

• 1 na 522 była próbą phishingu.

Zarządzane usługi poczty e-mail będą prawdopodobnie bardziej efektywne niż korzystanie z wewnętrznego oprogramowania antywirusowego, ponieważ usługodawcy są ekspertami w tej dziedzinie. Będą również w stanie szybciej identyfikować ataki robaków pocztowych i reagować na nie. Podsumowując, organizacje potrzebują opracowania zasad korzystania z oprogramowania antywirusowego. Powinno to określać:

1 Preferowane oprogramowanie antywirusowe, które ma być używane na wszystkich komputerach.

2 Częstotliwość i mechanizm aktualizacji oprogramowania antywirusowego.

3 Częstotliwość, z jaką cały komputer użytkownika końcowego jest skanowany w poszukiwaniu wirusów.

4 Organizacyjne blokowanie załączników z nietypowymi rozszerzeniami.

5 Organizacyjne wyłączanie makr w aplikacjach biurowych.

6 Skanowanie, które ma być wykonywane na serwerach pocztowych podczas pierwszego odbioru wiadomości e-mail i przed wysłaniem wirusów.

7 Zalecenia dotyczące korzystania z oprogramowania filtrującego spam.

8 Mechanizmy tworzenia kopii zapasowych i odzyskiwania.

Szkolenie personelu w zakresie identyfikowania różnych typów wirusów, a następnie reagowania na nie, może również ograniczyć wpływ wirusów. Oprócz robaków internetowych, które są uruchamiane automatycznie, można podjąć pewne kroki w celu zmniejszenia ryzyka związanego ze wszystkimi typami wirusów określonych powyżej. Następnie można opracować ogólne instrukcje w ramach polityki zmniejszania ryzyka infekcji i przeniesienia wirusa. Wiele z nich dotyczy również komputerów domowych:

1 Nie wyłączaj maszyn, gdy dyskietka nadal znajduje się w napędzie (zmniejsza transmisję napędów sektora startowego). Komputery PC można również skonfigurować tak, aby nie uruchamiały się ze stacji dyskietek.

2 Nie otwieraj załączników do wiadomości e-mail od osób, których nie znasz (ogranicz przenoszenie wirusów załączników do wiadomości e-mail). Ponieważ niektóre wirusy będą wysyłane z zaufanych źródeł, otwieraj tylko te załączniki, które wyglądają na uzasadnione, na przykład dokumenty Word z odpowiednimi nazwami. Niektóre wirusy używają rozszerzeń plików, które nie są powszechnie używane, takie jak .pif, .scr lub .vbs. Wyświetlanie dokumentów zamiast otwierania ich do edycji może również zmniejszyć ryzyko transmisji.

3 Pobieraj oprogramowanie wyłącznie z oficjalnego źródła i zawsze sprawdzaj, czy nie ma wirusów przed zainstalowaniem oprogramowania (zmniejsza ryzyko wystąpienia wirusów koni trojańskich).

4 Wyłącz lub wyłącz makra w programie Word lub Excel, chyba że używasz ich regularnie (zmniejsza ryzyko makrowirusów).

5 Codziennie twórz kopie zapasowe ważnych plików, jeśli ta funkcja nie jest wykonywana przez administratora systemu.

Kontrolowanie korzystania z usług informacyjnych

Problemy związane z kontrolowaniem usług informacyjnych zwykle wiążą się z jednym z dwóch problemów z punktu widzenia pracodawcy. Po pierwsze, zasoby sprzętowe i programowe przeznaczone do pracy są wykorzystywane do celów osobistych, co zmniejsza produktywność. Po drugie, monitorowanie wykorzystania informacji wprowadza prawne kwestie nadzoru. Monitorowanie wykorzystania usług informacyjnych obejmuje sprawdzanie:

• Wykorzystywanie poczty elektronicznej do celów osobistych.

• Niewłaściwe użycie poczty elektronicznej, które może prowadzić do działań prawnych przeciwko firmie.

• Korzystanie z Internetu lub witryn internetowych do użytku osobistego.

Problemy z używaniem poczty e-mail zostały omówione w dalszej części poświęconej zarządzaniu pocztą e-mail.

Monitorowanie komunikacji pracowników: Firmy monitorują personel e-maile i strony internetowe, do których uzyskują dostęp

Monitorowanie komunikacji elektronicznej

Monitorowanie lub nadzór komunikacji pracowników jest stosowany przez organizacje w celu zmniejszenia strat wydajności spowodowanych marnowaniem czasu. Czas można zmarnować, gdy członek personelu spędza czas, gdy otrzymuje wynagrodzenie, na sprawdzanie osobistych wiadomości e-mail lub uzyskiwanie dostępu do Internetu dla osobistych zainteresowań. Proste obliczenia wskazują na marnotrawstwo, gdy personel spędza czas na pracy nieprodukcyjnej. Jeśli pracownik zarabiający 25 000 funtów rocznie spędza 30 minut każdego dnia 5-dniowego tygodnia na odpowiadaniu na osobiste wiadomości e-mail lub odwiedzaniu witryn internetowych niezwiązanych z pracą, będzie to kosztować firmę ponad 1500 funtów rocznie. Dla firmy zatrudniającej 100 pracowników, w której przeciętny pracownik pracuje 46 tygodni w roku, oznacza to ponad 150 000 funtów rocznie lub koszt kilku nowych pracowników! Czynności, takie jak używanie mediów strumieniowych do przeglądania wiadomości lub pobierania klipów audio, mogą również obciążać sieci firmowe, jeśli są powszechne. Typowym przykładem rzekomego marnowania czasu, w którym firma zwolniła pracownika, była Lois Franxhi, 28-letni kierownik działu IT, który został zwolniony w lipcu 1998 r. Za wykonanie prawie 150 wyszukiwań w ciągu czterech dni w godzinach pracy podczas wakacji. Zażądała niesprawiedliwego zwolnienia - w

momencie zwolnienia była w ciąży. Podobnie jak w przypadku wielu niesłusznych zwolnień, sprawa nie była jasna, a pani Franxhi twierdziła, że firma zwolniła ją z powodu dyskryminacji ze względu na płeć. Trybunał odrzucił te roszczenia, stwierdzając, że pracownica kłamała na temat korzystania z Internetu, mówiąc, że używała go tylko przez jedną przerwę obiadową, podczas gdy w rzeczywistości zapisy wykazały, że korzystała z niego przez cztery dni. Niedawno DTI doniósł o pracowniku małej firmy usługowej, który miał dostęp do witryn internetowych dla dorosłych w pracy. Użył cudzego komputera, aby ukryć swoją aktywność. W innym przypadku, zakochany pracownik w średniej wielkości firmie spędzał do sześciu godzin dziennie na stronie internetowej agencji randkowej! Z badania wynika, że tym, co boli firmy, jest liczba tych incydentów, których doświadczają; średnio więcej niż jeden dzień. Chociaż mediana wyniosła tylko kilka incydentów w roku, niektóre małe firmy codziennie zgłaszały setki nadużyć związanych z pocztą elektroniczną Monitorowanie komunikacji pracowników może być również uzasadnione, jeśli wydaje się, że wysyłają lub odbierają wiadomości e-mail lub uzyskują dostęp do witryn internetowych zawierających treści organizacja uważa za niedopuszczalne. Typowymi przykładami takich treści są materiały pornograficzne lub rasistowskie. Jednak niektóre organizacje blokują nawet dostęp do witryn z wiadomościami, sportami lub e-mailami z powodu ilości czasu, jaki personel spędza na uzyskiwaniu do nich dostępu. Aby zdefiniować dozwoloną zawartość, wiele organizacji ma teraz zasady dopuszczalnego użytkowania. Na przykład wiele uniwersytetów, przy logowaniu się lub w laboratoriach komputerowych i bibliotekach ma powiadomienia o „zasadach dopuszczalnego użytkowania". Opisuje rodzaje materiałów, do których dostęp jest niedopuszczalny, a także jest sposobem na wyjaśnienie procedur monitorowania.

Skanowanie i filtrowanie to dwie najpopularniejsze formy monitorowania. Oprogramowanie do skanowania identyfikuje treść wysłanych lub odebranych wiadomości e-mail oraz odwiedzonych stron internetowych. Narzędzia takie jak WebSense lub MailMarshal SMTP firmy Marshal lub Web Marshal będą szukać konkretnych słów lub obrazów - na przykład pornografię wskazują odcienie skóry. Zostaną również ustalone reguły, na przykład blokujące załączniki do wiadomości e-mail o określonym rozmiarze lub zawierające przekleństwa, jak pokazano na rysunku 11.22. Takie narzędzia mogą również dać obraz najpopularniejszych typów witryn lub treści. Może to na przykład pokazać, ile czasu marnuje się na dostęp do serwisów informacyjnych i sportowych. Takie oprogramowanie zwykle ma również możliwości blokowania lub filtrowania. Oprogramowanie filtrujące, takie jak Websense (www.websense.com), może wykrywać i blokować inne działania, takie jak:

• Udostępnianie plików peer-to-peer (P2P), na przykład plików audio MP3

• Komunikatory internetowe za pomocą Yahoo! Messenger lub Microsoft Instant Messenger

• Wykorzystanie mediów strumieniowych (np. Audio i wideo) oraz innych aplikacji o dużej przepustowości

• Dostęp do określonych witryn, np. Niestety, niektóre firmy blokują wszelki dostęp do sieci społecznościowych lub serwisów informacyjnych, takich jak www.bbc.co.uk lub www.msn.co.uk, ponieważ analizy wykazały, że pracownicy spędzają z nimi bardzo dużo czasu. Dostęp do osobistych programów pocztowych, takich jak Yahoo! Mail lub Hotmail również mogą być blokowane. To nie byłoby popularne na uniwersytetach!

• Oprogramowanie szpiegujące, które ma na celu wysyłanie informacji zebranych z komputerów

• Programy typu adware, które umieszczają reklamy lub wyskakujące okienka

• Włamanie do pracowników

Zasady dopuszczalnego użytkowania: opis działań pracowników obejmujących korzystanie z komputerów w sieci, których kierownictwo nie uznało za dopuszczalne.

Oprogramowanie do skanowania: identyfikuje dostęp do poczty e-mail lub strony internetowej narusza wytyczne firmy lub zasady dopuszczalnego użytkowania.

Oprogramowanie filtrujące: oprogramowanie, które blokuje określone treści lub działania

Websense i podobne produkty mogą blokować witryny w różnych kategoriach, dla różnych typów pracowników, zgodnie z polityką dopuszczalnego użytkowania stosowaną przez organizację korzystającą z bazy danych (www.websense.com/products/about/database/categories.cfm), która zawiera ponad 1,5 miliona witryn internetowych w wielu kategoriach, z których tylko kilka podajemy w celu zilustrowania stopnia kontroli dostępnej dla pracodawcy. Przykładowe kategorie obejmują:

• Aborcja lub Pro-Choice lub Pro-Life

• Materiał dla dorosłych

• Kategoria dla rodziców, która zawiera kategorie: Treści dla dorosłych, Bielizna i strój kąpielowy, Nagość, Seks, Edukacja seksualna

• Treść dla dorosłych

• Grupy rzecznicze

• Biznes i ekonomia

• Dane i usługi finansowe

• Narkotyki

• Edukacja

• Zabawa

• Hazard

• Gry

• Rząd

• Obiekty wojskowe sponsorowane przez oddziały lub agencje sił zbrojnych

• Witryny organizacji politycznych sponsorowane przez partie polityczne i grupy interesu lub zawierające informacje o nich, które koncentrują się na wyborach lub ustawodawstwie

• Zdrowie

• Technologia informacyjna

• Wyszukiwarki i portale - na przykład strony obsługujące przeszukiwanie sieci, gazet i portali społecznościowych

• Poczta e-mail w sieci WWW - witryny obsługujące pocztę e-mail w sieci WWW

• Poszukiwania pracy

• Wojowniczość i ekstremista

• Wiadomości i media

• Rasizm i nienawiść

• Religia

• Zakupy

• Organizacje zawodowe i pracownicze

• Społeczeństwo i style życia

• Zainteresowania

• Randki i Randki

• Sporty

• Podróż

• Pojazdy

• Przemoc

• Bronie.

Zastanów się, ile z wymienionych powyżej osób możesz odwiedzić podczas studiów, w pracy lub w domu. Okaże się, że pracodawca, jeśli sobie tego życzy, może zablokować praktycznie każdą witrynę. Znam niektóre organizacje w Wielkiej Brytanii, które blokują dostęp do wszystkich witryn z wiadomościami i pracowałem w organizacji, która nawet blokowała dostęp do wyszukiwarek, takich jak Google, i poczty internetowej, takich jak Hotmail i Yahoo! Poczta. Kiedy wyszukiwarki są zablokowane, pracownicy na stanowiskach kierowniczych będą prawdopodobnie mieli ograniczone rozumienie środowiska biznesowego i nie będą mieli możliwości samorozwoju! Pracownicy prawdopodobnie negatywnie postrzegają pracodawcę, który nie ufa im w rozsądnym wykorzystaniu czasu.

Ocena wpływu: ocena procesu monitorowania pracowników w miejscu pracy w celu zidentyfikowania ulepszeń minimalizujących naruszenie prywatności pracowników.

Ukryte monitorowanie: monitorowanie, które pracodawca podejmuje bez powiadamiania personelu.

Przepisy dotyczące monitorowania pracowników

Chociaż monitorowanie pracowników wchodzi w zakres europejskiego prawa o ochronie danych, ustawa o ochronie danych nie została pierwotnie opracowana tak, aby obejmowała monitorowanie pracowników. Aby pomóc w wyjaśnieniu prawa dotyczącego monitorowania pracowników w Wielkiej Brytanii, w czerwcu 2003 r. Biuro Komisarza ds. Informacji opublikowało „Monitoring w pracy", trzecią część Kodeksu ochrony danych w zakresie praktyk zatrudnienia. Kodeks zawiera praktyczne wskazówki dla pracodawców, w jaki sposób powinni podejść do monitorowania pracowników w miejscu pracy. Te wytyczne mają na celu osiągnąć równowagę między pragnieniem pracowników w zakresie prywatności a potrzebą wydajnego prowadzenia działalności przez pracodawców. Kodeks nie zapobiega monitorowaniu, ale opiera się na koncepcji proporcjonalności. Proporcjonalność oznacza, że wszelkie niekorzystne skutki monitorowania muszą być uzasadnione korzyściami dla pracodawcy i innych osób. Dotyczy to oczywistej anomalii polegającej na tym, że prawo o ochronie danych odnosi się do indywidualnej zgody na przetwarzanie danych osobowych „dobrowolnie" i wyrażanie takiej zgody przez pracowników nie jest normalne. Kodeks wyjaśnia, że indywidualna zgoda nie jest wymagana, pod

warunkiem że organizacja przeprowadziła „ocenę wpływu" działań monitorujących. Zgodnie z kodeksem ocena skutków obejmuje:

• wyraźne określenie celu (celów) rozwiązania dotyczącego monitorowania i korzyści, jakie prawdopodobnie przyniesie

• określenie wszelkich prawdopodobnych niekorzystnych skutków ustaleń dotyczących monitorowania

• rozważenie alternatyw dla monitoringu lub różnych sposobów jego prowadzenia

• biorąc pod uwagę obowiązki wynikające z monitorowania

• ocena, czy monitorowanie jest uzasadnione.

Kodeks nie zawiera konkretnych zaleceń dotyczących monitorowania e-maili lub ruchu internetowego, ale odnosi się do nich jako do typowych działań monitorujących, które, jak sugeruje, mogą być dopuszczalne, jeśli personel zostanie o nich poinformowany i zostanie przeprowadzona ocena skutków. Kodeks prosi pracodawców o rozważenie, czy alternatywy mogą być lepsze niż systematyczne monitorowanie. Alternatywy mogą obejmować szkolenie lub wyraźną komunikację ze strony kierowników i analizę przechowywanych wiadomości e-mail w przypadku podejrzenia, że doszło do naruszenia, zamiast ciągłego monitorowania. Na przykład automatyczne monitorowanie jest preferowane zamiast przeglądania osobistych e-maili pracowników przez personel IT. Kodeks wyjaśnia również, że firma nie powinna podejmować żadnego ukrytego monitorowania; dlatego powinno być otwarte na temat wszystkich rodzajów monitorowania, które mają miejsce. Na uniwersytetach, jak wspomniano powyżej, przy logowaniu się lub w laboratoriach komputerowych i bibliotekach często pojawia się informacja o „polityce dopuszczalnego użytkowania". Opisuje rodzaje materiałów, do których dostęp jest niedopuszczalny, a także jest sposobem na wyjaśnienie procedur monitorowania. Wydaje się, że gdyby pracownik został ukarany dyscyplinarnie lub zwolniony za wysłanie np. Zbyt wielu osobistych e-maili, miałby uzasadnione podstawy do odwołania się, gdyby nie został poinformowany, że ma miejsce monitoring, a ich kierownicy nie wyjaśnili była dopuszczalną praktyką. W innych krajach europejskich obowiązują różne przepisy dotyczące monitorowania. Niektóre, takie jak Niemcy, są znacznie bardziej restrykcyjne niż Wielka Brytania pod względem poziomu monitorowania, jaki organizacje są w stanie przeprowadzić. Organizacje otwierające biura za granicą muszą być świadome lokalnych różnic w ograniczeniach prawnych dotyczących monitorowania pracowników i ochrony danych.

Spam: niechciana poczta e-mail (zwykle rozsyłana masowo i nieukierunkowana).

Botnet: niezależne komputery podłączone do Internetu są używane razem, zazwyczaj do złośliwych celów, poprzez oprogramowanie sterujące. Na przykład mogą być wykorzystywane do wysyłania spamu lub do ataku typu „odmowa usługi", w którym wielokrotnie uzyskują dostęp do serwera w celu pogorszenia jego usług. Komputery są często początkowo infekowane wirusem, gdy nie są stosowane skuteczne środki antywirusowe.

Zarządzanie pocztą e-mail

Poczta e-mail jest obecnie podstawowym narzędziem komunikacji biznesowej i jest również szeroko stosowana do użytku osobistego. Popularność poczty elektronicznej jako narzędzia komunikacji spowodowała, że każdego dnia wysyłano miliardy wiadomości. Dla osób fizycznych zarządzanie tą komunikacją w ich skrzynce e-mailowej szybko staje się niemożliwe! W przypadku menedżera usług informacyjnych, a nawet każdego menedżera biznesowego, istnieją trzy główne kontrole, które należy

wziąć pod uwagę, aby zmniejszyć ilość czasu efektywnie marnowanego przez personel czytający e-maile. Kontrole można wprowadzić jako część polityki zarządzania pocztą e-mail, aby zminimalizować ilość:

1 Spam (niechciana poczta e-mail).

2 Wewnętrzna poczta biznesowa.

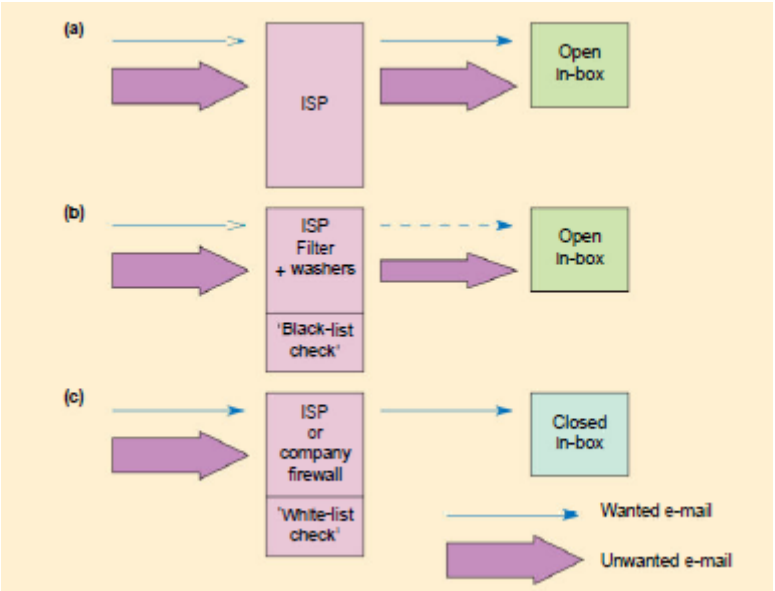
3 Zewnętrzna poczta biznesowa.

4 Osobisty e-mail (przyjaciele i rodzina).

Pomimo potencjalnej straty czasu spowodowanej niewłaściwym wykorzystaniem wiadomości e-mail, ankieta AMA sugeruje, że tylko 34% pracodawców prowadzi pisemną politykę przechowywania i usuwania wiadomości e-mail. Ponadto istnieją kwestie dotyczące odpowiedzialności prawnej za to, co pracownicy mówią w swoich wiadomościach e-mail, które również należy wziąć pod uwagę. Po kolei przyjrzymy się ryzyku i kontrolom każdego ryzyka związanego z pocztą elektroniczną.

1 Minimalizacja spamu (niechciana poczta e-mail)

Spam jest obecnie potencjalnym problemem dla każdej firmy i każdej osoby korzystającej z Internetu. W chwili pisania tego tekstu ponad 75% wiadomości e-mail było związanych ze spamem lub wirusami w niektórych krajach, a osoby, których skrzynki odbiorcze nie są chronione, mogą codziennie otrzymywać setki wiadomości spamowych. Spamerzy polegają na wysyłaniu milionów e-maili często z botnetów zainfekowanych komputerów w nadziei, że nawet przy odpowiedzi wynoszącej zaledwie 0,01% mogą zarobić trochę pieniędzy, jeśli niekoniecznie się wzbogacą. Środki prawne służące zwalczaniu spamu odniosły ograniczony sukces. Dlatego wielu menedżerów usług informacyjnych korzysta obecnie z szeregu metod kontrolowania spamu. Rysunek podsumowuje alternatywne techniki zwalczania spamu.



Rysunek (a) przedstawia oryginalną sytuację, w której cała poczta jest wpuszczana do skrzynki odbiorczej. Rysunek (b) wykorzystuje różne techniki w celu zmniejszenia ilości wiadomości e-mail poprzez identyfikację i blokowanie spamu. Rysunek (c) to zamknięta skrzynka odbiorcza, w której do organizacji są wpuszczane tylko znane, zaufane wiadomości e-mail. Pełen zakres technik, które można łączyć w celu zwalczania spamu, obejmuje:

1 Unikaj zbierania adresów Spamerzy przechwytują wiadomości e-mail z adresów e-mail publikowanych na stronach internetowych, a nawet kod programu używany do konwersji treści formularza online na wiadomość e-mail do firmy. Zmniejszając liczbę publikowanych adresów e-mail lub zmieniając ich format, można zmniejszyć liczbę adresów e-mail.

2 Poinformuj pracowników, aby nie odpowiadali na spam. Najgorszą rzeczą, jaką dana osoba może zrobić po otrzymaniu spamu, jest odpowiedź na skargę lub próba anulowania subskrypcji. To jedynie potwierdza spamerowi, że adres jest prawidłowy i prawdopodobnie wyśle więcej wiadomości-śmieci i sprzedadzą Twój adres innym spamerom. W programie Microsoft Outlook obrazy nie są włączone, ponieważ pobieranie obrazów w wiadomości e-mail w formacie HTML jest dla spamerów znakiem, że Twój adres jest prawidłowy.

3 Użyj filtrów. Oprogramowanie filtrujące może identyfikować spam na podstawie słów kluczowych i fraz, takich jak „Za darmo", „Seks" lub „Viagra", zawartych w temacie, na podstawie adresu i treści wiadomości e-mail. Filtry poczty e-mail są dostępne dla użytkowników poczty internetowej, takich jak Hotmail i Yahoo! Poczta z wiadomościami e-mail umieszczonymi w folderze wiadomości-śmieci. Microsoft Outlook Express ma własny filtr. Można również zainstalować oprogramowanie filtrujące, takie jak Mailryer (www.mailryer.net), Mcaffee Spamkiller (www.mcaffee.com). Niestety wielu spamerów wie, jak unikać słów kluczowych w filtrach. Problem z filtrami i innymi usługami polega na tym, że mogą istnieć „fałszywe alarmy" lub prawidłowe wiadomości e-mail, które są klasyfikowane jako śmieci. Ponadto spamerzy znajdują sposoby obejścia filtrów, umieszczając „gobbeldy gook" w stopce swoich wiadomości, które nie są rozpoznawane przez filtry, lub używając wariantów słów, takich jak Viagra czy Via-gra. Przegląd tych może być nadal konieczny. Technikę tę przedstawia rysunek (b).

4 Użyj „usług blokowania peer-to-peer". Wykorzystują one fakt, że ludzie są dobrzy w identyfikowaniu spamu, a następnie powiadamianiu centralnego serwera, który przechowuje indeks całego spamu. CloudMark (www.cloudmark.com), rozwiązanie peer-to-peer, wymaga od użytkowników identyfikowania spamu poprzez naciśnięcie przycisku „Zablokuj" w programie Outlook Express, który następnie aktualizuje serwer centralny, aby inni pobierali tę samą wiadomość w późniejszym czasie , jest automatycznie identyfikowany jako spam. Technikę tę przedstawia rysunek (b).

5 Użyj usług czarnej listy. Czarne listy to listy znanych spamerów, takich jak ci zgłoszeni do Spamhaus Project (www.spamhaus.com) lub SpamCop (www.spamcop.net). Są często używane w połączeniu z filtrami do blokowania wiadomości e-mail. Jeden z najczęściej używanych systemów opracowanych przez firmę Brightmail (www.brightmail.com) wykorzystuje globalną sieć adresów e-mail skonfigurowanych w celu wychwytywania i identyfikowania spamu. Brightmail jest coraz częściej używany przez dostawców usług internetowych, takich jak BT OpenWorld, do blokowania spamu, ale nie jest to tania usługa, która kosztuje od 5 do 15 USD rocznie. Cenę tę można łatwo uzasadnić oszczędnością czasu personelu w ciągu roku. Ta technika jest również przedstawiona na rysunku (b).

6 Korzystaj z usług białej listy. Metoda białej listy nie została powszechnie przyjęta, ponieważ jest trudna do skonfigurowania, ale prawdopodobnie oferuje najlepszą okazję na przyszłość. Coraz większym problemem dla firm korzystających z poczty elektronicznej w celach marketingowych są „fałszywe alarmy" - polegające na tym, że filtry identyfikują ich legalne wiadomości jako spam. Usługi białej listy są jednym z rozwiązań tego problemu. Biała lista zawiera listę prawdziwych adresów e-mail, z którymi prawdopodobnie będą chciały się skontaktować osoby w organizacji. Obejmuje wszystkich pracowników, partnerów, klientów i dostawców, którzy uzyskali zgodę pracowników na otrzymywanie wiadomości e-mail. E-maile od osób spoza listy będą blokowane. Jednak prowadzenie takiej listy będzie wymagało nowego oprogramowania i nowych procedur zapewniających jej aktualność. Jednym z podejść, które zostało opracowane w USA, jest koncepcja „wysyłającego za zgodą" opracowana przez

firmę Ironport (www.bondedsender.com). Nadawcy wiadomości e-mail z opcją zgody przesyłają zobowiązanie finansowe, aby udowodnić, że są renomowaną firmą. Inną usługą, która szybko zyskuje akceptację, jest Habeas (www.habeas.com), gdzie w poczcie wychodzącej wysyłany jest specjalny tekst („znak nakazu"), który umożliwia systemom filtrującym identyfikację wiadomości e-mail jako „nie spam". Technikę tę przedstawia rysunek (c). Dostawcy tacy jak Sendmail (www.sendmail.com), GoodMail (www.goodmail.com) oraz DomainKeys sponsorowany przez Yahool i Sender Policy Framework sponsorowany przez firmę Microsoft opracowali „technologię uwierzytelniania nadawcy", która umożliwia organizacjom weryfikację źródła wiadomości przed zaakceptowaniem go, automatycznie sprawdzając, czy pochodzi z miejsca, w którym twierdzi, że tak. Kolejnym podejściem jest wyzwanie / odpowiedź. W tym przypadku, jeśli wiadomość zostanie odebrana od osoby, która nie znajduje się na białej liście, do tej osoby zostanie wysłana wiadomość z prośbą o kliknięcie łącza w celu sprawdzenia, czy jest prawdziwą osobą, a nie spamerem (spamerzy nie mieliby czasu na zweryfikuj wszystkie adresy, ponieważ nie można tego zrobić automatycznie). Oczywiście stanowi to problem dla legalnych komercyjnych sprzedawców poczty e-mail.

7 Upewnij się, że oprogramowanie antywirusowe i blokowanie są skuteczne. Wirusy pocztowe są coraz częściej wykorzystywane przez spamerów, ponieważ są one metodą zbierania adresów e-mail. Ochrona przed wirusami musi być codziennie aktualizowana nowymi sygnaturami, jeśli adresy nie mają być przechwytywane przez wirusy.

Filtr poczty e-mail: oprogramowanie używane do identyfikowania spamu na podstawie jego cech, takich jak słowa kluczowe.

Czarna lista: zbiór znanych źródeł spamu używanych do blokowania poczty e-mail.

Biała lista: zbiór zaufanych źródeł wiadomości e-mail, które mogą wejść do skrzynki odbiorczej.

System wyzwań / odpowiedzi: e-mail z nieznanego źródła jest kwestionowany przez inny e-mail, który służy do udowodnienia, że nadawca jest prawidłowym nadawcą

2 Minimalizacja wewnętrznej firmowej poczty e-mail

Łatwość i niski koszt wysyłania wiadomości e-mail na listę dystrybucyjną lub kopiowania osób w wiadomości może sprawić, że każda osoba w organizacji będzie codziennie otrzymywać wiele wiadomości od współpracowników w organizacji. Ten problem jest zwykle gorszy w dużych organizacjach, po prostu dlatego, że każda osoba ma większą książkę adresową współpracowników. Komunikat prasowy British Computer Society podsumowujący badania przeprowadzone przez Henley Management College, opublikowany 20 grudnia 2002 r., Sugeruje, że menedżerowie tracą dużo czasu na przetwarzanie nieistotnych wiadomości e-mail. Zasugerował, że „brytyjskie kierownictwo odczuwa teraz ostry stres z powodu„ przeciążenia informacją "" z kierownictwem, „narzekając, że jest zalewany przez e-maile, które wymagają średnio dwóch godzin dziennie na zarządzanie"; Szczególnie frustrujące jest to, że prawie jedna trzecia otrzymanych wiadomości e-mail jest uznawana za nieistotną, a wiele z nich ma niską jakość. Dalsze ustalenia obejmowały:

• Spośród siedmiu typowych zadań zarządczych spotkania trwały średnio 2,8 godziny, drugie miejsce zajmowało poczta elektroniczna ze średnią 1,7 godziny, a dostęp do informacji z Internetu zajmował kolejne 0,75 godziny.

• Respondenci podali, że otrzymywali średnio 52 e-maile dziennie, a 7% otrzymywało 100 lub więcej e-maili dziennie.

• Menedżerowie podali, że mniej niż połowa e-maili (42 procent) wymagała odpowiedzi, 35 procent przeczytano tylko w celach informacyjnych, a prawie jedna czwarta została natychmiast usunięta. Średnio tylko 30% wiadomości e-mail zostało sklasyfikowanych jako istotne, 37% jako ważne, a 33% jako nieistotne lub niepotrzebne.

• Pomimo zastrzeżeń co do jakości i ilości otrzymywanych e-maili, większość ankietowanych (81 proc.) Uznała e-maile za technologię komunikacyjną, która miała najbardziej pozytywny wpływ na sposób wykonywania pracy, obok internetu i telefon komórkowy.

Aby przezwyciężyć tego rodzaju nadużywanie biznesowej poczty e-mail, firmy zaczynają opracowywać zasady dotyczące poczty elektronicznej, które wyjaśniają najlepsze praktyki. Na przykład, biorąc pod uwagę sposób, w jaki autorzy Chaffey and Wood używają poczty elektronicznej, szybko opracowaliśmy następujące wytyczne:

• Wysyłaj e-maile tylko do pracowników, w przypadku których konieczne jest poinformowanie lub podjęcie działań;

• Zakazywanie niektórych rodzajów e-maili, takich jak klasyczne e-maile do osoby siedzącej obok Ciebie lub osób w tym samym biurze (chociaż istnieją mocne argumenty przemawiające za tym, ponieważ e-mail jest nośnikiem asynchronicznym, a koledzy są nie zawsze dostępne lub nie chcą, aby im przeszkadzano);

• Unikaj „płonących" - są to agresywne e-maile, w których często wyrażane są uczucia, których nie można by powiedzieć twarzą w twarz. Jeśli otrzymasz irytującą wiadomość e-mail, najlepiej poczekać 10 minut, aż ostygnie, zamiast „podpalać" nadawcę;

• Unikaj „trolli" - to rodzaj e-maili blisko spokrewniony z e-mailami ognistymi. Są to posty do grupy dyskusyjnej celowo opublikowane w celu „zamknięcia" odbiorcy. Najlepiej je ignorować;

• Łączenie elementów z oddzielnych wiadomości e-mail w ciągu dnia lub tygodnia w jedną wiadomość e-mail na dzień / tydzień;

• Napisz jasne tematy;

• Strukturyzuj wiadomości e-mail tak, aby można je było szybko skanować za pomocą podtytułów oraz list numerowanych i wypunktowanych;

• Jasno określić działania następcze;

• Czytając wiadomości e-mail, używaj folderów do klasyfikowania wiadomości e-mail według treści i priorytetu;

• Odczytuj e-maile i sprawdzaj ich partiami, np. raz dziennie lub po południu, zamiast być powiadamianym i otwierać każdy przychodzący e-mail;

• Usuń wiadomości e-mail, które nie są potrzebne do przyszłego wykorzystania (duże ilości są przenoszone na serwery przez personel, który nie usuwa wiadomości e-mail i ich załączników);

• I tak dalej - wszystkie wskazówki dotyczące zdrowego rozsądku, ale często zdrowy rozsądek nie jest powszechny!

3 Minimalizacja zewnętrznej firmowej poczty e-mail

Oprócz spamu, który jest niechciany i zazwyczaj nieukierunkowany, osoby w organizacji mogą również otrzymywać wiele e-maili od legalnych dostawców. Na przykład kierownik działu IT może otrzymywać

e-maile od producentów sprzętu i oprogramowania, usługodawców, organizatorów wydarzeń lub konferencji oraz biuletyny elektroniczne z czasopism. Te źródła wiadomości e-mail zwykle nie są kontrolowane przez zasady firmy dotyczące poczty e-mail; wybór odpowiednich biuletynów elektronicznych jest zwykle pozostawiony indywidualnej decyzji pracownika. Technologie blokowania wiadomości e-mail, takie jak filtry antyspamowe, zazwyczaj nie blokują takich wiadomości, ale prymitywne filtry mogą blokować takie słowa, jak „Oferta" lub „Bezpłatne", które również pojawiają się w legalnych wiadomościach biznesowych. System wezwań / odpowiedzi będzie nadal umożliwiał otrzymywanie takich e-maili. Ponadto dostępna jest technologia opisana w rozdziale 12, która blokuje dostęp do niektórych witryn internetowych, takich jak serwisy informacyjne lub rozrywkowe, a to oprogramowanie zmniejsza skuteczność biuletynów elektronicznych, ponieważ obrazy nie są pobierane z zablokowanych witryn. Podejście stosowane przez wiele osób w celu pomocy w kontrolowaniu informacji z tych źródeł polega na korzystaniu z oddzielnego adresu e-mail z głównej skrzynki odbiorczej podczas rejestracji. Może to być Hotmail lub Yahoo! Adres pocztowy i tę formę e-newslettera można odczytać w biurze lub w domu, a także przy zmianie pracy.

4 Minimalizowanie osobistych wiadomości e-mail (przyjaciele i rodzina)

Chociaż istnieje wiele ankiet dotyczących ilości spamu i ilości czasu spędzonego na przetwarzaniu wiadomości e-mail w pracy, publikowanych jest stosunkowo niewiele danych dotyczących czasu spędzonego na pisaniu osobistych wiadomości e-mail. Większość z nich nie jest niezależna; jest zlecany przez sprzedawców oprogramowania do monitorowania korzystania z poczty elektronicznej. Jednak używanie poczty elektronicznej do użytku osobistego będzie miało miejsce, jeśli nie będzie środków, aby go powstrzymać. Aby zminimalizować ten problem i niektóre problemy związane z nadmiernym wykorzystaniem poczty e-mail do celów biznesowych, można podjąć następujące kroki:

1 Stworzyć pisemne wytyczne określające zasady dotyczące dopuszczalnego korzystania z poczty elektronicznej oraz procedury dyscyplinarne w przypadku naruszenia wytycznych;

2 Stosować rosnące poziomy kontroli lub sankcji za naruszenia, w tym przeglądy wyników, ostrzeżenia słowne, usunięcie przywilejów e-mailowych, rozwiązanie umowy i działania prawne;

3 Zapewnienie szkolenia dla personelu w zakresie akceptowalnego i efektywnego korzystania z poczty elektronicznej;

4 Monitoruj e-maile pod kątem podpisów osobistego użytku i wszelkich naruszeń polityki, np. przeklinać i odpowiednio zareagować.

Hacking: proces uzyskiwania nieautoryzowanego dostępu do systemów komputerowych, zwykle w sieci

Hakerstwo

„Hakowanie" odnosi się do procesu uzyskiwania nieautoryzowanego dostępu do systemów komputerowych, zwykle w sieci. Hakowanie może przybierać różne formy. Hakowanie w celu uzyskania korzyści finansowych ma zwykle na celu kradzież tożsamości, w przypadku gdy dane osobowe i dane karty kredytowej są dostępne w celu oszustwa. Hakowanie może również mieć miejsce w złym zamiarze. Na przykład były pracownik może uzyskać dostęp do sieci w celu usunięcia plików lub przekazania informacji konkurentowi. Niektórzy z notorycznych hakerów, którzy byli ścigani, ale często wydaje się, że ostatecznie wygrali na swoich wykroczeniach, to:

• Robert Morris - syn głównego naukowca w amerykańskim National Computer Security Center, ten magistrant stworzył w 1988 r. destrukcyjnego robaka internetowego, który wykorzystał lukę w

zabezpieczeniach systemu operacyjnego Unix. Po uruchomieniu spowodował awarię tysięcy komputerów . Zakłócenie było częściowo przypadkowe i wydał instrukcje dla administratorów systemu, jak rozwiązać problem. Został skazany na trzy lata w zawieszeniu, 400 godzin pracy społecznej i grzywnę w wysokości 10 050 dolarów. Obecnie jest adiunktem na MIT, gdzie pierwotnie wypuścił swojego robaka, aby ukryć jego stworzenie na Uniwersytecie Cornell.

• Kevin Poulsen - W 1990 roku Poulsen przejął wszystkie linie telefoniczne stacji radiowej KIIS-FM w Los Angeles, zapewniając, że będzie 102. rozmówcą. Poulsen wygrał Porsche 944 S2. Był to jeden z wielu włamań przeprowadzonych, gdy pracował w dzień dla firmy SRI International, a nocą włamał się. W końcu został wytropiony, a w czerwcu 1994 r. przyznał się do siedmiu zarzutów związanych z pocztą, oszustwami teleinformatycznymi i komputerowymi, praniem pieniędzy i utrudnianiem wymiaru sprawiedliwości, skazany na 51 miesięcy więzienia i zapłacenie 56 000 dolarów odszkodowania. To był najdłuższy wyrok, jaki kiedykolwiek wydano za włamanie. Obecnie jest dziennikarzem zajmującym się bezpieczeństwem komputerowym.

• Kevin Mitnick - Mitnick, pierwszy haker, który pojawił się na plakacie FBI „Most Wanted", został aresztowany w 1995 roku. Później przyznał się do czterech oszustw, dwóch oszustw komputerowych i jednego nielegalnego przechwycenia komunikacji przewodowej. . Przyznał, że włamał się do systemów komputerowych i ukradł autorskie oprogramowanie Motoroli, Novella, Fujitsu, Sun Microsystems i innych firm. Został skazany na 46 miesięcy. Po zdaniu wyroku został konsultantem ds. Bezpieczeństwa, a obecnie jest czołowym komentatorem na temat bezpieczeństwa, a także wielokrotnie występował w telewizji, pisał książki i artykuły.

• Vladimir Levin - absolwent matematyki, który był członkiem rosyjskiego gangu, który rzekomo zorganizował oszustwo Citibank za 10 milionów dolarów. Aresztowany przez Interpol na londyńskim lotnisku Heathrow w 1995 roku.

• Alexey Ivanov - Akt oskarżenia przeciwko Iwanowowi z czerwca 2001 r., W którym zarzucano, że uzyskał nieautoryzowany dostęp do CTS Network Services, dostawcy usług internetowych z siedzibą w San Diego. Iwanow rzekomo wykorzystał skradziony numer karty kredytowej do otwarcia konta w CTS, a gdy już znalazł się w komputerach firmy, włamał się do systemów, aby przejąć kontrolę nad komputerami. Następnie użył komputerów CTS do przeprowadzenia serii ataków komputerowych na firmy handlu elektronicznego, w tym dwa procesory kart kredytowych - Sterling Microsystems z Anaheim i Transmark z Rancho Cucamonga - oraz NaraBank z Los Angeles. Iwanow rzekomo ukradł informacje finansowe klientów, takie jak numery kart kredytowych i kont bankowych, co doprowadziło do oszustwa o wartości 25 milionów dolarów. Skazano na trzy lata więzienia.

Hakowanie może nie być bezpośrednio związane z kradzieżą lub uszkodzeniem, ale uzyskanie dostępu do systemu może być postrzegane przez hakera jako wyzwanie techniczne. Termin „hacking" tradycyjnie odnosi się do procesu tworzenia kodu programu, innej formy wyzwania technicznego. Można to niemal uznać za rozrywkę, choć nieetyczną. Chociaż hakowanie nie jest tak popularne jak oglądanie sportu, w każdym kraju występuje więcej niż jedna lub dwie osoby. BBC (2003) donosi, że TruSecure, amerykańska organizacja monitorująca hakowanie, obecnie śledzi ponad 11 000 osób w około 900 różnych grupach i gangach hakerskich.

Inżynieria społeczna: wykorzystywanie ludzkich zachowań w celu uzyskania dostępu do informacji o zabezpieczeniach komputera od pracowników lub osób

Można zidentyfikować trzy główne formy uzyskiwania nieuprawnionego dostępu do systemów komputerowych. po pierwsze, można użyć normalnych punktów wejścia do systemów poprzez nazwy użytkowników i hasła. Na przykład wiele loginów do systemu ma domyślnie nazwę użytkownika

„administrator”. Czasami hasło będzie takie samo. Inne popularne hasła to dni tygodnia lub ames dzieci. Dostępne są narzędzia do wypróbowania różnych alternatywnych metod logowania, chociaż większość nowoczesnych systemów odmówi dostępu po kilku próbach. Hakowanie można połączyć z kradzieżą tożsamości, aby zorientować się, jakie hasła są używane. Druga forma hakowania wykorzystuje znane luki w systemach. Chociaż te luki w systemach operacyjnych, takich jak Windows lub Linux lub przeglądarkach internetowych, takich jak Internet Explorer, są publicznie znane i zostaną opublikowane w witrynie internetowej producenta i specjalistycznych witrynach bezpieczeństwa, będzie wielu administratorów systemów, którzy nie zaktualizowali swoich systemów za pomocą najnowsza aktualizacja zabezpieczeń lub „łatka”. Wynika to częściowo z faktu, że istnieje tak wiele luk w zabezpieczeniach, a nowe są ogłaszane co tydzień. Po trzecie, Kevin Mitnick odnosi się do „inżynierii społecznej”, która zazwyczaj polega na podszywaniu się pod pracowników organizacji w celu uzyskania dostępu do szczegółów bezpieczeństwa. Przykładem tego, podanym w pracy Mitnick i Simon (2002), jest sytuacja, w której osoba atakująca kontaktuje się z nowym pracownikiem i informuje go o konieczności przestrzegania zasad bezpieczeństwa. Atakujący następnie prosi użytkownika o podanie hasła, aby sprawdzić, czy jest ono zgodne z polityką wyboru hasła trudnego do odgadnięcia. Gdy użytkownik ujawni swoje hasło, dzwoniący wydaje zalecenia dotyczące konstruowania przyszłych haseł w taki sposób, aby osoba atakująca mogła je odgadnąć.

Zapora: wyspecjalizowane oprogramowanie zwykle instalowane na serwerze w miejscu, w którym firma ma połączenie z Internetem. Jego celem jest zapobieganie nieautoryzowanemu dostępowi do firmy

Etyczny haker: haker zatrudniony legalnie do testowania jakości bezpieczeństwa systemu.

Ochrona systemów komputerowych przed hakerami

Ochrona systemów komputerowych przed hakerami polega na stworzeniu środków przeciwdziałających trzem głównym typom hakowania przedstawionym powyżej. Aby uzyskać dostęp do systemów za pomocą haseł, można opracować zasady zmniejszające ryzyko dostępu. Jednym prostym podejściem jest wymaganie, aby nowe hasła były wymagane co miesiąc i zawierały co najmniej jedną cyfrę oraz kombinację wielkich i małych liter. Zapobiega to używaniu przez użytkowników prostych haseł, które można łatwo odgadnąć. Edukacja jest niezbędna, aby zmniejszyć ryzyko fałszywie uzyskanych haseł za pomocą „inżynierii społecznej”, ale to nigdy nie wyeliminuje całkowicie zagrożenia. Systemy komputerowe można również chronić, ograniczając dostęp w miejscu, w którym sieć zewnętrzna wchodzi do firmy. Zapory ogniowe są niezbędne, aby uniemożliwić dostęp do poufnych informacji firmowych z zewnątrz, zwłaszcza w przypadku utworzenia ekstranetu. Firewalle są zwykle tworzone jako oprogramowanie montowane na oddzielnym serwerze w miejscu, w którym firma jest podłączona do Internetu. Oprogramowanie zapory można wtedy skonfigurować tak, aby akceptowało łącza tylko z zaufanych domen reprezentujących inne biura w firmie. Należy również wprowadzić środki uniemożliwiające dostęp do systemów poprzez opublikowane luki w zabezpieczeniach. BBC (2003) podała, że w 2003 roku istniało 5500 luk w zabezpieczeniach, które można było wykorzystać. Wymagane są również zasady dotyczące aktualizowania systemów operacyjnych i innego oprogramowania do najnowszych wersji. Wykonywanie wszystkich aktualizacji jest niepraktyczne, ale nowe luki muszą być monitorowane i poprawki do kategorii najwyższego ryzyka. Jest to zadanie specjalistyczne i często zlecane na zewnątrz. TruSecure (www.trusecure.com) to przykład specjalistycznej firmy, która monitoruje luki w zabezpieczeniach i doradza organizacjom w zakresie zapobiegania. TruSecure szacuje, że tylko 80 lub 90 procent luk jest używanych regularnie, więc poprawki powinny mieć na nich priorytet. TruSecure świadczy usługę dla setek organizacji, aby sprawdzić, czy mają te luki w zabezpieczeniach. Zatrudniają również zespół ludzi, którzy próbują infiltrować grupy hakerów w celu ustalenia najnowszych technik. TruSecure przekazało FBI ponad 200

dokumentów dotyczących autora wirusa „Melissa”. Chociaż nie znali jego prawdziwego imienia, znali jego trzy aliasy i stworzyli jego szczegółowy profil. Kolejnym podejściem stosowanym przez organizacje do sprawdzania zabezpieczeń przed hakerami jest zatrudnianie „etycznych hakerów”. Są to byli hakerzy, którzy teraz wykorzystują swoje umiejętności do testowania luk w istniejących systemach. Chociaż wszystkie powyższe przykłady hakowania dotyczą sieci komputerowych, czasami można również zastosować techniki „mało zaawansowane”. Guardian (2003) opisał przypadki, w których przestępcy podszywali się pod pracowników call center w celu uzyskania dostępu do kont klientów!

Bezpieczne transakcje e-commerce

W przypadku e-firm oferujących sprzedaż online istnieją również dodatkowe zagrożenia bezpieczeństwa z punktu widzenia klienta lub sprzedawcy:

(a) Dane transakcji lub dane karty kredytowej skradzione podczas transportu.

(b) Dane karty kredytowej klienta skradzione z serwera sprzedawcy.

(c) Sprzedawca lub klient nie jest tym, za kogo się podaje.

W tej sekcji oceniamy środki, które można podjąć, aby zmniejszyć ryzyko takich naruszeń bezpieczeństwa handlu elektronicznego. Zaczynamy od przeglądu teorii bezpieczeństwa w Internecie, a następnie przeglądamy zastosowane techniki.

Zasady bezpiecznych systemów

Zanim przyjrzymy się zasadzie bezpiecznych systemów, warto przejrzeć standardową terminologię dla różnych stron zaangażowanych w transakcję:

• Kupujący. Są to konsumenci kupujący towary.

• Kupcy. Są to sprzedawcy.

• Urząd certyfikacji (CA). Jest to organ wydający certyfikaty cyfrowe potwierdzające tożsamość kupujących i handlowców.

• Banki. To są tradycyjne banki.

• Wydawca tokenów elektronicznych. Wirtualny bank, który wydaje walutę cyfrową.

Podstawowe wymagania dotyczące systemów bezpieczeństwa z różnych stron transakcji są następujące:

1 Uwierzytelnienie - czy strony transakcji się podają (ryzyko (c) powyżej)?

2 Prywatność i poufność - czy dane transakcji są chronione? Konsument może chcieć dokonać anonimowego zakupu. Czy wszystkie nieistotne ślady transakcji są usuwane z sieci publicznej, a wszystkie zapisy pośredniczące są wyeliminowane (ryzyka (b) i (c) powyżej)?

3 Integralność - sprawdza, czy wysłana wiadomość jest kompletna, tj. Czy nie jest uszkodzona.

4 Niezaprzeczalność - zapewnia, że nadawca nie może odmówić wysłania wiadomości.

5 Dostępność - jak wyeliminować zagrożenia dla ciągłości i wydajności systemu?

Certyfikaty cyfrowe (klucze): składają się z kluczy złożonych z dużych liczb, które służą do jednoznacznej identyfikacji osób.

Szyfrowanie symetryczne: obie strony transakcji używają tego samego klucza do kodowania i dekodowania wiadomości.

Szyfrowanie asymetryczne: obie strony używają powiązanego, ale innego klucza do kodowania i dekodowania wiadomości

Podpisy cyfrowe: metoda identyfikacji osób lub firm przy użyciu szyfrowania z kluczem publicznym.

Certyfikaty i urzędy certyfikacji (CA): Certyfikat jest ważny jako kopia klucza publicznego osoby lub organizacji wraz z informacjami identyfikacyjnymi. Jest wydawany przez zaufaną stronę trzecią (TTP) lub urząd certyfikacji (CA). Urzędy certyfikacji udostępniają klucze publiczne, a także wydają klucze prywatne.

Podejścia do tworzenia bezpiecznych systemów

Certyfikaty cyfrowe

Istnieją dwie główne metody szyfrowania przy użyciu certyfikatów cyfrowych.

1 Szyfrowanie z kluczem tajnym (symetryczne) Szyfrowanie symetryczne polega na tym, że obie strony mają identyczny (wspólny) klucz, który jest znany tylko im. Tylko ten klucz może być używany do szyfrowania i odszyfrowywania wiadomości. Tajny klucz musi zostać przekazany od jednej strony do drugiej przed użyciem w taki sam sposób, jak kopia bezpiecznego klucza do skrzynki załączników musiałaby zostać wysłana do odbiorcy informacji. Takie podejście tradycyjnie było używane do osiągnięcia bezpieczeństwa między dwoma oddzielnymi stronami, takimi jak duże firmy prowadzące EDI. Tutaj klucz prywatny jest wysyłany drogą elektroniczną lub kurierem, aby zapewnić, że nie zostanie skopiowany. Ta metoda nie jest praktyczna w przypadku ogólnego handlu elektronicznego, ponieważ dla kupującego nie byłoby bezpieczne przekazanie sprzedawcy tajnego klucza, ponieważ utraciłby nad nim kontrolę i nie można go było następnie wykorzystać do innych celów. Sprzedawca musiałby również zarządzać wieloma kluczami klientów.

2 Szyfrowanie z kluczem publicznym (asymetryczne)

Szyfrowanie asymetryczne jest tak zwane, ponieważ klucze używane przez nadawcę i odbiorcę informacji są różne. Te dwa klucze są powiązane kodem numerycznym, więc tylko para kluczy może być używana w połączeniu do szyfrowania i odszyfrowywania informacji. Rysunek pokazuje, jak działa szyfrowanie kluczem publicznym w kontekście handlu elektronicznego.

Klient może złożyć zamówienie u sprzedawcy, automatycznie wyszukując klucz publiczny sprzedawcy, a następnie używając tego klucza do zaszyfrowania wiadomości zawierającej jego zamówienie. Zaszyfrowana wiadomość jest następnie przesyłana przez Internet i po otrzymaniu przez sprzedawcę jest odczytywana przy użyciu klucza prywatnego sprzedawcy. W ten sposób tylko sprzedawca, który ma jedyną kopię klucza prywatnego, może odczytać zamówienie. W odwrotnym przypadku sprzedawca mógłby potwierdzić tożsamość klienta, odczytując informacje o tożsamości, takie jak

podpis cyfrowy zaszyfrowany kluczem prywatnym klienta przy użyciu jego klucza publicznego. Pretty Good Privacy (PGP) to system szyfrowania z kluczem publicznym używany do szyfrowania wiadomości e-mail.

Podpisy cyfrowe

Podpisy cyfrowe mogą być wykorzystywane do tworzenia systemów komercyjnych przy użyciu szyfrowania klucza publicznego w celu uzyskania uwierzytelnienia: sprzedawca i kupujący mogą udowodnić, że są autentyczni. Cyfrowy podpis kupującego jest szyfrowany przed wysłaniem wiadomości przy użyciu jego klucza prywatnego, a po otrzymaniu klucz publiczny kupującego jest używany do odszyfrowania podpisu cyfrowego. To dowodzi, że klient jest autentyczny. Podpisy cyfrowe nie są obecnie powszechnie stosowane ze względu na trudności związane z konfigurowaniem transakcji, ale staną się bardziej rozpowszechnione wraz ze stabilizacją infrastruktury klucza publicznego (PKI) i wzrostem wykorzystania urzędów certyfikacji.

Infrastruktura klucza publicznego (PKI) i urzędy certyfikacji (CA)

Aby podpisy cyfrowe i szyfrowanie za pomocą klucza publicznego były skuteczne, konieczne jest upewnienie się, że klucz publiczny przeznaczony do odszyfrowania dokumentu faktycznie należy do osoby, która Twoim zdaniem przesyła Ci dokument. Rozwijającym się rozwiązaniem tego problemu jest wydanie przez zaufaną stronę trzecią (TTP) wiadomości zawierającej informacje identyfikacyjne właściciela oraz kopię klucza publicznego tej osoby. TTP są zwykle nazywane „urzędami certyfikacji" (CA), a rolę tę prawdopodobnie pełnią różne organy, takie jak banki i poczta. Ta wiadomość nazywa się „certyfikatem". W rzeczywistości, ponieważ szyfrowanie asymetryczne jest raczej powolne, często jest to tylko próbka wiadomości, która jest szyfrowana i używana jako reprezentatywny podpis cyfrowy. Przykładowe informacje o certyfikacie mogą obejmować:

• dane identyfikacyjne użytkownika;

• identyfikacja organu wydającego i podpis cyfrowy;

• klucz publiczny użytkownika;

• data ważności tego certyfikatu;

• klasa certyfikatu;

• cyfrowy kod identyfikacyjny tego certyfikatu.

Proponuje się, aby istniały różne klasy certyfikatów w zależności od rodzaju zawartych informacji. Na przykład:

• imię i nazwisko, adres e-mail

• prawo jazdy, numer ubezpieczenia społecznego, data urodzenia

• sprawdzenie zdolności kredytowej

• specyficzne dla organizacji dane poświadczenia bezpieczeństwa.

Wirtualna sieć prywatna: Sieć prywatna utworzona przy użyciu infrastruktury sieci publicznej Internetu.

Secure Sockets Layer (SSL): Powszechnie stosowana technika szyfrowania do szyfrowania danych przesyłanych przez Internet z przeglądarki internetowej klienta na serwer internetowy sprzedawcy.

Secure Electronic Transaction (SET): standard szyfrowania z kluczem publicznym, mający na celu umożliwienie bezpiecznych transakcji e-commerce, rozwój potencjalnych klientów przez MasterCard i Visa

Wirtualne sieci prywatne

Wirtualna sieć prywatna (VPN) to prywatna sieć rozległa działająca w sieci publicznej, a nie droższa sieć prywatna. Technika, za pomocą której działa VPN, jest czasami nazywana tunelowaniem ”i obejmuje szyfrowanie zarówno nagłówków pakietów, jak i treści przy użyciu bezpiecznej formy protokołu internetowego znanego jako IPSec. Jak wyjaśniono w rozdziale 3, VPN umożliwiają globalnej organizacji bezpieczne prowadzenie działalności, ale przy użyciu publicznego Internetu zamiast droższych, zastrzeżonych systemów.

Aktualne podejście do bezpieczeństwa handlu elektronicznego

W tej sekcji omawiamy podejścia stosowane przez witryny handlu elektronicznego w celu osiągnięcia bezpieczeństwa przy użyciu technik opisanych powyżej.

Protokół Secure Sockets Layer (SSL)

SSL to protokół bezpieczeństwa, pierwotnie opracowany przez firmę Netscape, ale obecnie obsługiwany przez wszystkie przeglądarki, takie jak Microsoft Internet Explorer. SSL jest używany w większości transakcji e-commerce B2C, ponieważ jest łatwy w obsłudze dla klienta bez konieczności pobierania dodatkowego oprogramowania lub certyfikatu. Kiedy klient wchodzi do bezpiecznego obszaru płatności w witrynie handlu elektronicznego, używany jest protokół SSL, a klient jest informowany, że „masz zamiar przeglądać informacje przez bezpieczne połączenie”, a do oznaczenia tego zabezpieczenia używany jest symbol klucza. Podczas szyfrowania zauważą, że prefiks adresu internetowego w przeglądarce zmienia się z chttp: // ”na„ https: // ”, a na dole okna przeglądarki pojawia się kłódka. Jak protokół SSL odnosi się do różnych koncepcji bezpieczeństwa opisanych powyżej? Główne udogodnienia, jakie zapewnia to bezpieczeństwo i poufność. SSL umożliwia utworzenie prywatnego łącza między klientem a sprzedawcą. Szyfrowanie służy do zaszyfrowania szczegółów transakcji e-commerce, gdy jest ona przekazywana między nadawcą a odbiorcą, a także gdy szczegóły są przechowywane na komputerze na każdym końcu. Przechwycenie takiej wiadomości i jej odszyfrowanie wymagałoby zdecydowanej próby. SSL jest szerzej stosowany niż konkurencyjna metoda S-HTTP. Szczegółowe etapy SSL są następujące:

1 Przeglądarka klienta wysyła żądanie bezpiecznego połączenia.

2 Serwer odpowiada certyfikatem cyfrowym, który jest wysyłany w celu uwierzytelnienia.

3 Klient i serwer negocjują klucze sesji, które są kluczami symetrycznymi używanymi tylko na czas trwania transakcji.

Ponieważ przy wystarczającej mocy obliczeniowej, czasie i motywacji możliwe jest odszyfrowanie wiadomości zaszyfrowanych przy użyciu protokołu SSL, wiele wysiłku wkłada się w znalezienie bezpieczniejszych metod szyfrowania, takich jak SET. Z punktu widzenia handlowca istnieje również problem polegający na tym, że uwierzytelnienie klienta nie jest możliwe bez uciekania się do innych metod, takich jak sprawdzenie zdolności kredytowej.

Urzędy certyfikacji (CA)

W celu zapewnienia bezpiecznego handlu elektronicznego istnieje wymóg zarządzania ogromną liczbą kluczy publicznych. Zarządzanie to obejmuje procedury i protokoły niezbędne przez cały okres

generowania, rozpowszechniania, unieważniania i zmiany klucza, wraz z funkcjami administracyjnymi oznaczania czasu / daty i archiwizacji. Pomyślne utworzenie urzędu certyfikacji jest ogromnym wyzwaniem związanym z budowaniem zaufania i złożonym zarządzaniem. Istnieją dwa przeciwstawne poglądy na temat sposobu sprostania temu wyzwaniu:

• Zdecentralizowane: kierowane rynkiem, tworzące „wyspy zaufania" oparte na marce, takie jak Stowarzyszenie Konsumentów. Istnieje praktyczna potrzeba, aby lokalne fizyczne biuro przedstawiało certyfikaty o potwierdzonej wartości, np. paszporty, prawa jazdy. Banki i poczta mają ogromną przewagę.

• Scentralizowane: w Wielkiej Brytanii Departament Handlu i Przemysłu (DTI) zaproponował hierarchiczne drzewo prowadzące ostatecznie do rządu.

Najbardziej znanym komercyjnym urzędem certyfikacji jest Verisign (www.verisign.com) i jest on powszechnie używany do weryfikacji handlowców. Na przykład witryna Avon korzysta z Verisign, aby udowodnić swoim klientom, że jest oryginalną witryną. Urzędy pocztowe i dostawcy usług telekomunikacyjnych działają również jako CA. Przykłady w Wielkiej Brytanii to BT (Trust Wise) i poczta (ViaCode).

Uspokajanie klienta

Po wprowadzeniu środków bezpieczeństwa zawartość witryny sprzedawcy może być wykorzystana do uspokojenia klienta, na przykład Amazon (www.amazon.com) poważnie traktuje obawy klientów dotyczące bezpieczeństwa, oceniając ich znaczenie i ilość treści, które temu poświęca kwestia. Niektóre z zastosowanych podejść wskazują na dobre praktyki w łagodzeniu obaw klientów. Obejmują one:

• wykorzystanie gwarancji klienta w celu zabezpieczenia zakupu;

• jasne wyjaśnienie zastosowanych środków bezpieczeństwa SSL;

• podkreślenie rzadkości oszustw („dziesięć milionów klientów dokonało bezpiecznych zakupów bez oszustw związanych z kartami kredytowymi");

• korzystanie z alternatywnych mechanizmów zamawiania, takich jak telefon lub faks;

• eksponowanie informacji w celu rozwiania obaw - gwarancja jest jedną z głównych opcji menu.

Firmy mogą również korzystać z niezależnych stron trzecich, które ustalają wytyczne dotyczące prywatności i bezpieczeństwa w Internecie. Najbardziej znanymi organizacjami międzynarodowymi są TRUSTe (www.truste.org) i Verisign do uwierzytelniania płatności (www.verisign.com). W poszczególnych krajach mogą istnieć inne organy, takie jak w Wielkiej Brytanii ISIS lub program Zakupy internetowe to bezpieczne (http://isis.imrg.org)

Podsumowanie

1 Analiza wymagań biznesowych i wymagań użytkowników dotyczących systemów e-biznesu jest ważna w dostarczaniu użytecznych i odpowiednich systemów.

2 Modelowanie procesów służy do oceny istniejących procesów biznesowych i sugerowania poprawionych procesów. Techniki, takie jak analiza zadań i wykresy procesów przepływu pracy z projektowania przepływu pracy, są przydatne w zrozumieniu zadań, które muszą być obsługiwane przez system, i słabości w bieżącym procesie.

3 Modelowanie danych dla systemów e-biznesu obejmuje głównie tradycyjne podejście do relacji między podmiotami.

4 Projekty architektoniczne obejmują ocenę odpowiedniej integracji między starszymi systemami a nowymi systemami handlu elektronicznego. Takie projekty są oparte na podejściu klient-serwer.

5 Projekt interfejsu użytkownika można ulepszyć, stosując ustrukturyzowane podejścia, takie jak przypadki użycia i postępując zgodnie z ewoluującymi standardami dotyczącymi struktury serwisu, struktury strony i zawartości.

6 Projekt bezpieczeństwa jest ważny dla utrzymania zaufania wśród bazy klientów. Rozwiązania zabezpieczające mają na celu ochronę serwerów przed atakami i zapobiegają przechwytywaniu wiadomości podczas ich przesyłania.