Old Man GURU Magazine

Wychodzi bardzo nieregularnie, kiedy wydaje mi się,
że mam coś ciekawego lub pożytecznego do napisania...

Numer 8/2010 **24 marzec 2010 r.**

Interfejs Użytkownika - czy to proste? *(ciąg dalszy)*

Jak już wspomniałem podczas badania potrzeb użytkownika musimy uważać, aby były one zgodne z realizowanymi przez niego zadaniami. Często będziemy mieli do czynienia z próbami ich zafałszowania:

"*Mój komputer jest wyposażony w nagrywarkę DVD, która jest mi niezbędna*"!

Należy wówczas postawić pytania - "a w jakim celu? Jakie zadania wymagają od Pani (Pana) nagrywania płyt DVD (CD)? Jakie zbiory są nagrywane na płyty? Co się dzieje z nagranymi płytami? W jaki sposób i gdzie są przechowywane?"...

Przecież są to elementarne pytania ze strony każdego, kto zajmuje się zarządzaniem bezpieczeństwem informacji - bo bez nadzoru nad danymi, które opuszczają system informacyjny nie może być mowy o żadnym zarządzaniu. Oczywiście, mogą istnieć (nieliczne!) przypadki, w których zachodzi potrzeba nagrywania płyt na typowym stanowisku roboczym - lecz musi to być objęte odpowiednimi zapisami w Polityce Bezpieczeństwa systemu - a więc odpowiedź na powyższe pytania powinna być oczywista i wynikać wprost z tych zapisów. Oczywiście te same uwagi dotyczą urządzeń odczytujących płyty CD/DVD i popularnych pamięci FLASH USB!

Możliwa sytuacja, w której użytkownik będzie się starał ukryć przez audytorem faktycznie realizowane czynności - najczęściej mamy wówczas do czynienia ze zjawiskiem zwanym "Computer Missuse" - czyli wykorzystywaniem służbowego komputera do zadań nie wynikających z obowiązków służbowych - choćby przeglądania zdjęć zrobionych przez koleżankę w czasie wakacji. Użytkownicy nie traktują takich czynności jako zagrożenia dla pracy systemu - a tym czasem nic bardziej błędnego - nie można w ogóle mówić o zarządzaniu bezpieczeństwem informacji, jeśli dopuszczamy do gromadzenia w systemie zbiorów, o których nic nie wiemy! A przecież dysk komputera biurkowego czy notebooka po podłączeniu ich do sieci może być łatwo widoczny! Jeśli znajdą się na nim zbiory nieznanego pochodzenia, to znaczny wzrost zagrożenia jest oczywisty. Nie można także nie brać pod uwagę zwiększonego obciążenia sieciowego systemu tworzenia kopii awaryjnych - zbiory użytkowników to zazwyczaj spore zbiory multimedialne.

Poprawnie przeprowadzona analiza potrzeb stanowiska pracy pozwoli na na zdefiniowanie takiego interfejsu użytkownika, który pozwoli mu na sprawną realizację powierzonych zadań - a równocześnie nie udostępni mu takich funkcji, które nie są mu do tego potrzebne.

Czy takie postępowanie jest uzasadnione? Jeśli mamy zamiar poważnie myśleć o zarządzaniu bezpieczeństwem informacji jest po prostu niezbędne! Wystarczy podać tylko proste argumenty:

W raporcie o wyciekach danych z systemów komputerowych za rok 2009 opublikowanym przez InfoWatch jedynie 51% odnotowanych wycieków danych powstało na skutek celowych działań. 43,5% wycieków powstało przypadkowo (w 5% nie stwierdzono tego jednoznacznie). Dane te zostały uzyskane z systemów nadzoru klasy DLP i potwierdzają tezę, że w znacznej części dane są upubliczniane w wyniku przypadku i bez złej woli. Nie zmienia to jednak faktu, że SĄ upubliczniane. Dzieje się to w wyniku błędów lub zapomnień ze strony użytkowników. Mogą one dotyczyć nie tylko obsługi samego komputera - ale również wynikać z bardzo prostych przeoczeń - pozostawieniu wydruku na drukarce, kartki w skanerze lub kserokopiarce - statystyki InfoWatch wskazują, że ponad 20% przypadków upublicznienia danych dotyczy kopii papierowych!!!
O ile z takim roztargnieniem walczyć jest dość trudno (w pewnym stopniu pomóc może ograniczenie dostępu do urządzeń) to poprawnie opracowany interfejs użytkownika może w bardzo dużym stopniu zaradzić błędom lub pomyłką podczas obsługi samego komputera. Przygotować taki interfejs w dowolnym systemie można w dość prosty sposób, jednak koniecznie trzeba wziąć pod uwagę kilka ważnych faktów:

Po pierwsze - komputer w firmie - to nie komputer w domu!

Być może niektórzy będą starali się protestować - jak to, przecież to taki sam sprzęt (Personal Computer), ten sam system operacyjny (nie ważne czy Windows, Linux czy MacOS) - to co je różni?

Różnica jest zasadnicza - bo za administrację komputera domowego odpowiada jego użytkownik (lub czasem sprawniejszy kolega, syn itp.). To sam użytkownik instaluje nowe programy, dba (lub częściej nie dba) o kopie awaryjne i inne systemy zabezpieczenia danych (personal Firewall, system antywirusowy itp.), kontroluje (przynajmniej powinien) czy transmisje z bankiem są odpowiednio bezpieczne (certyfikat strony, szyfrowanie itp.).

W przypadku komputera w firmie mającej choćby minimalne ambicje zarządzania bezpieczeństwem informacji takie postępowanie jest po prostu niedopuszczalne. Komputerem (a raczej stanowiskiem pracy zrealizowanym za pomocą komputera) musi bezwarunkowo zarządzać specjalista (pracownik działu IT zwany często informatykiem). To on jest odpowiedzialny za bezawaryjną i bezpieczną eksploatację systemu i to on decyduje (zgodnie z realizowanymi procesami biznesowymi) jakie programy ma do dyspozycji użytkownik, do jakich zasobów sieciowych posiada dostęp i jakie mechanizmy bezpieczeństwa są na komputerze (oraz w systemie) zaimplementowane. Użytkownik komputera firmowego powinien otrzymać gotowe i w pełni sprawne oraz bezpieczne środowisko pracy i za wyjątkiem dobrze uzasadnionych przypadków nie powinien mieć żadnych uprawnień niezbędnych do konfiguracji systemu (z układem ikon na ekranie włącznie), a już na pewno nie może decydować o funkcjonalności mechanizmów związanych z bezpieczeństwem danych.

Można to osiągnąć na wiele różnych sposobów, należy sobie jednak zdać sprawę z zadań, które będzie realizować dział IT organizacji.

Tworząc interfejs użytkownika na podstawie analizy potrzeb należy brać pod uwagę następujące czynniki:

Minimalizację możliwości popełnienia przypadkowego błędu. Można to uzyskać (między innymi) poprzez:

- *zastosowanie przejrzystego układu ograniczonej liczby właściwie rozmieszczonych ikon. Jak wynika z cytowanych w pierwszej części wyników badań ergonomicznych powinny być one umieszczane przede wszystkim w pierwszym górnym wierszu, a w drugiej kolejności z pierwszej (lewej) kolumnie.*
- *zabezpieczenie interfejsu (rozkładu ikon, systemów menu) przed przypadkową lub celową modyfikacją przez użytkownika. Wynika to z właściwości ludzkiej pamięci, która przesuwa często wykonywane zadania do pamięci długotrwałej, która zapewnia znacznie mniejszą stopę błędów oraz znaczne skrócenie czasu podejmowania decyzji wyboru.*
- *wprowadzenie programowej obsługi ewentualnych błędnych akcji - na przykład uruchomienia kilku kopii programów przez wielokrotne klikanie na ikonę (tak zwane "zabezpieczenie przed zaklikaniem").*
- *Uruchamianie stale wykorzystywanych programów użytkowych (np. obsługi sprzedaży) automatycznie przy starcie komputera (po dokonaniu uwierzytelnienia) - a następnie ich wybór za pomocą prostych skrótów klawiszowych. W przypadku systemów operacyjnych wyposażonych w takie możliwości polecane jest wykorzystywanie wielu konsoli - np. na stacji roboczej opracowanej na potrzeby Urzędów Skarbowych każda z pierwszych 4 konsoli jest przyporządkowana jednej aplikacji, a przełączanie się pomiędzy nimi następuje błyskawicznie za pomocą sekwencji <Ctrl><Alt>Fx (x oznacza tu numer konsoli). Redukuje to czas uzyskania dostępu do potrzebnej aktualnie aplikacji, ponieważ pracuje ona bez przerwy, a przełączane są jedynie standardowe wejścia i wyjścia.*

Poprawnie opracowany interfejs użytkownika zwiększa znacznie jego wydajność i minimalizuje liczbę popełnianych błędów, ponieważ jego obsługa przez użytkowników bardzo szybko staje się wręcz automatyczna. Wszelkie zmiany interfejsu użytkownika powinny być dokładnie przemyślane i ostrożnie wprowadzane, ponieważ wymagają czasu na przystosowanie się do nich użytkowników systemu. Znaczącemu zwiększeniu ulega też liczba popełnianych błędów i możliwa jest frustracja użytkowników, która wyraża się w tak zwanym "oporze materii".

Jak już wspomniałem poprawny interfejs użytkownika można utworzyć w każdym systemie operacyjnym - nawet bardzo ograniczonym - klasy Embedded System. Co więcej, z mojej wieloletniej praktyki wynika, że użytkownicy w bardzo wielu przypadkach nie są w stanie stwierdzić, jaki system operacyjny pracuje na ich stacji roboczej i wielokrotnie twierdzili np. że korzystają z "Windowsów" pracując tak naprawdę na stacji roboczej wykorzystującej system

Linux. Po prostu realizują swoje zadania (uruchamianie programów) dokładnie w taki sam sposób i nie jest dla nich istotne, czy program pracuje lokalnie czy też na odległym serwerze sieciowym.

Pracując na komputerze firmowym pracujemy korzystamy z sieci lokalnej. Powstaje więc pytanie, gdzie użytkownik powinien zapisywać i przechowywać swoje zbiory?

Z punktu widzenia osoby odpowiedzialnej za zarządzanie bezpieczeństwem informacji odpowiedź znów daje statystyka opublikowana w Raporcie InfoWatch, a dokładniej zestawienie źródeł, z których wyciekły informacje.

Źródło wycieku danych	Wycieki celowe	Wycieki przypadkowe
Komputery przenośne (notebooki, PDA itp.)	**15,7%**	**9,7%**
Przenośne nośniki danych (HDD, USB Flash, CD, DVD itp.)	2,1%	7,5%
Komputery biurkowe (desktop), podręczne serwery	**20,8%**	8,1%
Internet (bezpośrednio, bez poczty elektronicznej)	**17,9%**	**19,7%**
Kopie papierowe	7,2%	**35,9%**
Kopie archiwalne (w tym także awaryjne)	8,2%	4,7%
Poczta elektroniczna	2,9%	8,4%

Zarządzający bezpieczeństwem informacji powinni więc brać pod uwagę, że największe ryzyko wycieku celowego jest związane ze słabo zabezpieczonymi komputerami biurkowymi - zaś wycieku przypadkowego z brakiem procedur postępowania z kopiami papierowymi (Hard Copies).

Na drugim miejscu w obu przypadkach znalazła się sieć Internet, a na trzecim - komputery przenośne, jednak warto odnotować, że celowe przejęcia danych z komputerów przenośnych są o wiele częstsze, niż przypadkowe wycieki. Złodzieje informacji znacznie częściej interesują się kopiami awaryjnymi niż przenośnymi nośnikami danych pozostającymi w dyspozycji użytkowników (które z kolei są dość często po prostu gubione...).

Opublikowana statystyka jasno wskazuje, że zapobieganie kradzieży danych musi uwzględniać nieco inne priorytety ochrony niż eliminowanie wycieków przypadkowych.

Wycieki przypadkowe są powodowane głównie przez niezamierzone działania lub błędy szeregowych użytkowników systemu informacyjnego, a więc poprawne rozwiązanie interfejsu użytkownika i nie pozostawianie dostępu do funkcji, które nie są niezbędne dla wykonywania zadań służbowych w połączeniu z Polityką Bezpieczeństwa (postępowanie z kopiami papierowymi!) może znacznie ograniczyć liczbę tych wycieków.

Ciekawe jest również zestawianie typu danych, które podlegają wyciekom. Otóż zdecydowanie na pierwszym miejscu są tu dane osobowe (90% wycieków!). Wrażliwe dane komercyjne, "know-how" itp. to jedynie 3,5%, zaś tajemnice państwowe i wojskowe - 1,8%. Pozostałych typów danych nie udało się jednoznacznie zakwalifikować.

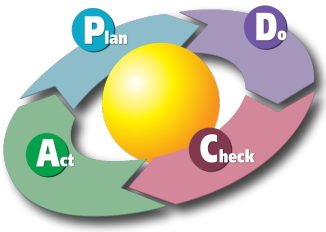
Ochrona danych osobowych powinna być więc absolutnym priorytetem. Niestety, w wielu przypadkach (zwłaszcza w mniejszych firmach komercyjnych) nie przykłada się do niej odpowiedniej wagi, pomimo obowiązywania większości krajów odpowiednich przepisów.

Kilka odnotowanych i wyjaśnionych spektakularnych przykładów z 2009 roku:

- USA: 76 mln rekordów Archiwów Narodowych (NARA) - źródło: dysk przekazany do naprawy bez wykonania operacji wipe.
- UK: 62 mln rekordów Ministerstwo Pracy - włamanie wewnętrzne przez pracowników.
- Niemcy: 7,5 mln rekordów serwisu StayFriends - włamanie zewnętrzne.
- UK: 6 mln rekordów rządowej bazy właścicieli samochodów - włamanie wewnętrzne.
- UK: 2,5 mln rekordów National Health Service (dane pacjentów) - włamanie zewnętrzne.
- Japonia: 1,5 mln rekordów bazy klientów firmy komercyjnej - włamanie wewnętrzne.
- USA: 807 tyś. rekordów bazy policyjnej - kradzież taśm z kopiami archiwalnymi.

Z danych osobowych zawartych w systemie korzysta często bardzo wielu jego użytkowników i jest to absolutnie niezbędne przy realizacji przez nich zadań służbowych. Konieczne jest więc przykładanie odpowiedniej wagi do procedur związanych z ich wykorzystywaniem oraz udostępnianiem. Dane te można bowiem korzystnie sprzedać - przykładem mogą być dane osobowe właścicieli samochodów w Wielkiej Brytanii (przykład powyżej), które zostały sprzedane koncernom motoryzacyjnym - udowodniono, że wykorzystała je w dystrybucji reklam firma Castrol. Rząd Republiki Federalnej Niemiec zdecydował się również na zakup skradzionych danych związanych z systemem podatkowym!

Jeśli pozostawimy użytkownikom znaczną swobodę w zapisywaniu i przechowywaniu zbiorów utrudnimy tym samych znacznie stworzenie SZBI. Użytkownicy mają bowiem tendencję do zapisu danych na dyskach lokalnych lub tworzenie ich kopii (elektronicznych lub papierowych) "na wszelki wypadek". Zapewnienie odpowiedniego bezpieczeństwa tych kopii może być trudne do zrealizowania - poza tym utrudni to organizację tworzenia i ochrony kopii awaryjnych. Tworząc interfejs użytkownika należy brać to pod uwagę.



Proces tworzenia interfejsu użytkownika to wręcz idealna ilustracja działań w Cyklu Deminga. Należy liczyć się z koniecznością sprawdzenia swoich pomysłów w praktyce oraz obserwacji akceptacji wprowadzonych rozwiązań przez użytkowników, a także przetestowania stabilności, odporności na ewentualne błędy - a także próby uzyskania dostępu do chronionych zasobów lub wręcz ataków!
Testowaniu należy również poddać system auditingu działań użytkownika jeśli taki system jest wykorzystywany.

Interfejs użytkownika jest jednym z kluczowych interfejsów systemu - o innych kluczowych interfejsach w dalszych numerach OldMan GURU.

