Romuald Swarcewicz

Zaufanie i pewność w e-biznesie (I)

Fot. Nick Benjaminsz

Zaufanie jest bardzo ważnym czynnikiem w kontaktach międzyludzkich, technologiach sieci informatycznych, a w szczególności w Internecie. Przeszkodą w powszechnym użyciu dostępnych technologii jest nie tylko konieczność pozyskania odpowiednich kwalifikacji i niezbędnego wsparcia technicznego, ale przede wszystkim brak zaufania do oferowanych rozwiązań.

Przeszkodą w powszechnym użyciu dostępnych technologii jest przede wszystkim brak zaufania do oferowanych rozwiązań.

Kupowanie w Internecie jest łatwiejsze, wygodniejsze i zajmuje mniej czasu niż kupowanie tradycyjne. Czy możemy jednak zaufać, iż dokonaliśmy zakupu na właściwej witrynie, że zakupiony towar dojdzie do nas zgodnie z przedstawionym opisem, że nikt nie podglądał danych naszej karty płatniczej że ktoś nie obserwuje naszych zakupów?

Od wszystkich komputerów i sieci telekomunikacyjnych oczekuje się pewnego poziomu ufności określonego warunkami bezpieczeństwa. A obecnie, kiedy stopniowo migrujemy z sieci przewodowych do radiowych, w których interfejs jest otwarty dla wszystkich, wymagania bezpieczeństwa są bardziej rygorystyczne.

Gdy zaufanie jest jednostronne, wówczas kooperacja nie może być efektywna. Rekomendacja odgrywa znaczącą rolę w zaufaniu.

Określenie „pewny" rozumiemy jako bezpieczny. W dziedzinie technologii informatycznej (IT) to określenie odnosi się do potrzeb biznesowych. Bezpieczeństwo IT przede wszystkim odnosi się do zabezpieczenia infrastruktury IT i informacji w przedsiębiorstwie.

Celem bezpiecznej technologii informatycznej jest umożliwienie organizacji wypełniania celów jej misji/przedsięwzięcia przy zapewnieniu uniknięcia ryzyka dla organizacji, jej partnerów i klientów. Wymagania bezpieczeństwa lub inaczej cele zabezpieczenia systematyzuje się następująco:

Dostępność. Dostępność systemu to cecha zapewniająca dostęp tylko uprawnionym użytkownikom. Ten warunek zabezpiecza przed: zamierzoną lub przypadkową próbą nieuprawnionego wymazania danych bądź też odmawia obsługi lub pokazania danych; próbą użycia systemu lub danych w niedozwolonym celu.

Integralność. W dziedzinie IT rozpatruje się ją z dwóch punktów widzenia: integralności danych i integralności systemu. Nieautoryzowana manipulacja danymi może mieć miejsce zarówno przy składowaniu, jak i w czasie przetwarzania lub transmisji. Integralność systemu oznacza, że system nie był manipulowany, a nawet dostępny w sposób nieuprawniony.

Poufność. W przypadku informacji danych i systemu oznacza, że tylko autoryzowani użytkownicy otrzymują informację i że jest ona zablokowana dla jednostek nieuprawnionych.

Wiarygodność. Wiarygodność jest wymaganiem unikalnego przeprowadzania działania przez jednostkę. Wymaganie to staje się coraz bardziej istotne, gdy wzrasta uzależnienie biznesu od IT. Wiarygodność jest znacząca dla takich zagadnień, jak niezaprzeczalność, fałszywe wydzielenie, wykrycie i zapobieganie włamaniu oraz odzyskanie stanu przed atakiem.

Pewność. Pewność to wymaganie wykazania, że przedsięwzięcia zabezpieczenia zostały właściwie zaimplementowane i sprawdzają się w działaniu oraz mają dostateczną odporność na umyślną próbę penetracji systemu.

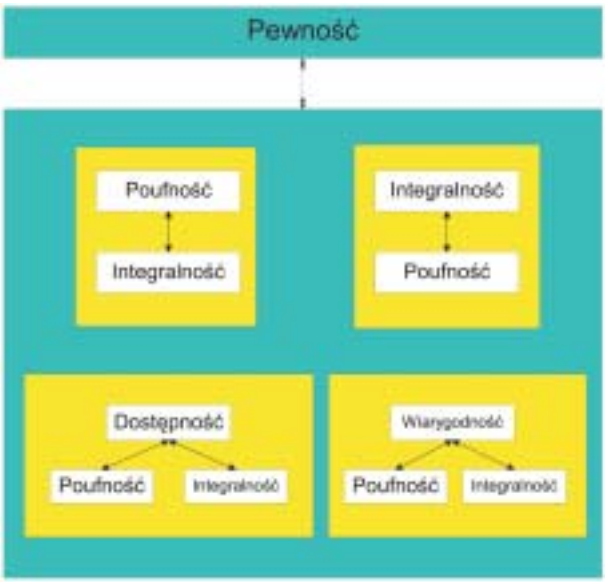
Te pięć celów zabezpieczenia jest ze sobą powiązanych i zależnych od siebie (rys.1).

Poufność nie może być osiągnięta, jeśli nie będzie zachowana integralność systemu i odwrotnie. Dostępność nie jest utrzymywana przez system, który nie wspiera poufności i integralności. Podobnie bez poufności nikt nie może mieć pewności swoich działań. Użytkownicy muszą mieć zapewnione, że system spełnia wymagania dostępności, integralności, zachowuje poufność i pewność.

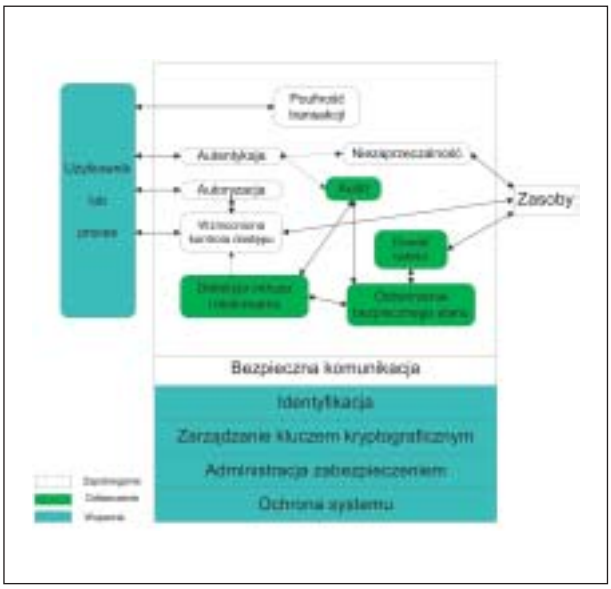
Model systemu zabezpieczenia (rys. 2) pokazuje relacje pomiędzy głównymi i pomocniczymi funkcjami. Podstawę modelu systemu bezpieczeństwa stanowią najbardziej ogólne funkcje wspomagające: prewencyjne i odtworzenia. Ich działanie koncentruje się na prewencji zabezpieczeń przed tym, co się wydarzy i wreszcie funkcje odtworzenia identyfikujące jakiekolwiek włamania i przywracające system do poprzedniego stanu.

Poniższe funkcje stanowią podstawę dla działania pozostałych

Identyfikacja. Odnosi się do utożsamienia wszystkich elementów systemu takich jak użytkownicy, procesy i zasoby informacji.



Rys.1. *Relacje między celami zabezpieczenia pewności*



Rys. 2. *Model funkcjonalny pewności zabezpieczeń*

Tab. Mapa celów i funkcji bezpieczeństwa

Cele bezpieczeństwa / Funkcje zabezpieczeń	Dostepność	Integralność	Poufność	Wiarygodność	Pewność
Identyfikacja		x	x	x	
Zarządzanie kluczem kryptograficznym		x	x	x	
Administracja zabezpieczeniem					x
Ochrona systemu					x
Bezpieczna komunikacja	x	x	x		
Autentyczność	x			x	
Autoryzacja	x	x	x	x	
Wzmocniona kontrola dostępu	x	x	x	x	x
Niezaprzeczalność				x	
Poufność transakcji			x		
Audit				x	
Detekcja intruza i powstrzymanie	x	x		x	x
Dowód całości	x	x		x	x
Odzyskiwanie stanu pewności	x	x		x	

Zarządzanie kluczem kryptograficznym identyfikuje obiekt w sposób bezpieczny.
Administracja bezpieczeństwem jest wymagana do implementowania nowych funkcji, aktualizacji istniejących i monitorowania operowania tych funkcji.
Ochrona systemu ogólnie przedstawia całkowite zaufanie implementacji technicznej. Przykładami są ochrona rezydującej informacji, separacji procesów, modularności i minimalizacji tego, do czego trzeba mieć zaufanie.

Funkcje prewencyjne zabezpieczają system przed włamaniami

Bezpieczna komunikacja pomiędzy komunikującymi się jednostkami. Zaufanie do komunikacji jest szczególnie istotne, gdy odbywa się ona w systemie dystrybucyjnym. Funkcja jest krytyczna, ponieważ tworzy bazę dla integralności, dostępności i poufności.
Autentykacja sprawdza czy obiekt jest tym, za kogo się podaje, czyli sprawdza tożsamość obiektu.
Autoryzacja jest kluczem zezwalającym obiektowi na zrobienie czegoś, może to być dostęp do zasobów, ekstra korzyści.
Wzmocniona kontrola dostępu powinna monitorować, jaki obiekt otrzymał dostęp w legalny sposób, co może robić a czego nie.
Niezaprzeczalność odnosi się do pewności, funkcja ta daje pewność, że nadawca nie może wyprzec się nadanej informacji, a odbiorca nie może zaprzeczyć otrzymania jej.
Poufność transakcji zabezpiecza prywatność cyfrowej transakcji. Wszystkie systemy: rządowe, korporacyjne i indywidualne coraz bardziej koncentrują się na zagadnieniu poufności.

Funkcje detekcji i odzyskiwania wykrywają włamanie i następnie przywracają stan poprzedni

Detekcja intruza i powstrzymanie. Te funkcje monitorują każde podejrzane zachowanie, które mogłoby naruszyć bezpieczeństwo systemu. Wczesne wykrycie intruza pozwala na podjęcie przedsięwzięć zabezpieczających system.
Dowód całości pozwala na wykrycie czy system lub dane są w całości.
Odzyskiwanie stanu pewności po tym jak zostanie wykryte włamanie.
Cele bezpieczeństwa można zestawić z funkcjami zabezpieczeń, jak pokazano to w tabeli.
Nie wszystkie funkcje są konieczne dla wszystkich celów, ale nie oznacza to, że funkcje, które nie będą bezpośrednio użyte, nie mogą być zignorowane. Zarządzanie kluczem kryptograficznym i identyfikacja są wymagane tylko dla integralności, poufności i wiarygodności, ale nie dla dostępności i pewności. Jednakże dostępność zależy od poufności i integralności, a pewność jest związana z czterema funkcjami. Tak więc słaba funkcja zarządzania kluczem będzie miała wpływ na wszystkie cele bezpieczeństwa.

W kolejnym numerze „e-Faktów" opublikujemy drugą część artykułu poświęconą metodom szyfrowania informacji.