**34. [rozszerzenie] – pojęcia związane z bezpieczeństwem informacji:**

Zgodnie z Polską Normą „Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji”, która jest polską wersją międzynarodowej normy ISO/IEC, **bezpieczeństwo informacji** „oznacza, że jest ona chroniona przed wieloma różnymi zagrożeniami w taki sposób, aby zapewnić ciągłość prowadzenia działalności, zminimalizować straty oraz maksymalizować zwrot nakładów na inwestycje i działania o charakterze biznesowym”. Informacja jest w pełni bezpieczna, jeśli zostaną zachowane wszystkie z poniższych elementów:

* **poufność** (*confidentiality*),
* **integralność** (*integrity*),
* **dostępność** (*availability*).

**Poufność** gwarantuje, że wszelkie informacje oznaczone jako np. tajne, prywatne czy poufne, będą chronione przed dostępem osób trzecich. Osoby trzecie to w tym wypadku wszelkie podmioty, które nie uzyskały autoryzacji dostępu do tych informacji [29].

Zagrożenia dla poufności mogą pochodzić z wielu różnych źródeł. Przykładowo, tajną informację wyświetlaną na monitorze CRT lub LCD można podsłuchać korzystając np. z receptorów Van Ecka [6]. Dzięki nim, istnieje możliwość odczytania wyświetlanych informacji, które nie są nawet zapisane na żadnym nośniku komputerowym. Innym przykładem może być niedbałe rozmieszczenie monitorów w pomieszczeniu. Nawet, jeśli znajduje się ono na dziesiątym piętrze, należy zwrócić uwagę na to, by poufne informacje nie mogły być dostrzeżone przy użyciu lornetki, bądź aparatu fotograficznego z odpowiednio dobranym obiektywem. Zupełnie innym zagrożeniem dla poufności może być używanie zbyt krótkiego hasła chroniącego poufne informacje.

Do ochrony poufnych informacji wykorzystuje się techniki takie, jak szyfrowanie danych, uwierzytelnienie, autoryzację a nawet wymaganie, by osoby mające styczność z takimi informacjami ściśle przestrzegały zapisów polityki bezpieczeństwa panującej w danej organizacji.

Jako, że pojęcia „uwierzytelnienie” oraz „autoryzacja” są często mylone (być może ze względu na ich angielskie tłumaczenia), poniżej zamieszczono ich krótkie wyjaśnienie. **Uwierzytelnienie** (*authentication*) to proces weryfikacji tożsamości podanej przez użytkownika bądź inny podmiot. Samo przedstawienie się systemowi informacyjnemu, np. poprzez podanie loginu danego podmiotu, nazywane jest **identyfikacją** (*identification*). Dopiero po identyfikacji, system poprzez np. sprawdzenie, czy użytkownik podaje właściwe dla danego loginu hasło, dokonuje uwierzytelnienia, dzięki któremu może stwierdzić, że użytkownik bądź inny podmiot jest faktycznie tym, za kogo się podaje. Natomiast **autoryzacja** (*authorization*) to przydzielanie użytkownikom określonych przywilejów, które pozwolą mu wykonywać pewne działania w systemie. Autoryzacji najczęściej dokonuje administrator systemu.

**Integralność** informacji, zwana czasem nienaruszalnością informacji, jest aspektem bezpieczeństwa dotyczącym ingerencji w treść przechowywanych danych. **O ile poufność oznaczała ochronę przed nieautoryzowanym dostępem do informacji, tak integralność oznacza ochronę przed nieautoryzowanym modyfikowaniem** zapisanych w systemie informacji, nieautoryzowanym **tworzeniem** informacji (np. w postaci nowych plików) oraz nieautoryzowanym **usuwaniem** informacji. Warto zaznaczyć, że **pojęcia poufności oraz integralności informacji są rozłączne**, tzn. utrata poufności nie oznacza jednocześnie utraty integralności, a utrata integralności nie oznacza utraty poufności. Przykładowo, utrata integralności może powstać w wyniku wprowadzenia szumów do transmisji danych, jednak bez odpowiednich urządzeń czy narzędzi, które mogłyby przechwycić transmitowane pakiety danych, nie ma możliwości uzyskania do nich dostępu. Tak więc poufność danych zostaje w tym przypadku zachowana. Podobnie, dzięki np. luce w aplikacji można mieć możliwość odczytu poufnych informacji, natomiast zaimplementowane metody ochrony mogą uniemożliwiać ich nieautoryzowaną modyfikację.

Zagrożeniami dla integralności danych mogą być zakłócenia transmisji, zarówno te zamierzone, wprowadzone przez intruza, bądź niezamierzone, wprowadzone do transmisji przez np. zewnętrzne pola elektromagnetyczne. Utrata integralności może nastąpić również wskutek tak prostych czynności jak przyłożenie odpowiednio silnego magnesu do dysku twardego przechowującego dane na nośniku magnetycznym. Innym przykładem zagrożenia dla integralności danych jest atak typu „man in the middle”.

Powszechnie używane funkcje haszujące mogą być przydatne, gdy należy upewnić się czy integralność przesyłanych czy przechowywanych danych została zachowana. Funkcje te przyjmują na wejście dowolnie długi ciąg danych, dając na wyjściu krótki (najczęściej o niezmiennej długości) ciąg znaków. Uruchamiając tego typu funkcję przed wysłaniem danych oraz po odebraniu ich przez odbiorcę można sprawdzić czy nie zostały one zmienione w trakcie transferu [20]. Mechanizmami stosowanymi do zapewnienia integralności są również funkcje uwierzytelniające, które sprawdzają czy podmiot chcący dokonać zmian w informacji ma do tego prawo, a także stosowanie korekcji błędów poprzez dodanie nadmiarowych (z punktu widzenia treści informacji) danych naprawczych.

Warto również zwrócić uwagę na dwa inne pojęcia, często używane zamiennie w stosunku do integralności danych. Pojęcia te to: **integralność** systemu (*system integrity*) oraz **spójność** (*consistency*). Nie oznaczają one jednak tego samego, co integralność danych. Integralność systemu można utożsamiać z wymaganiem nakładanym na system, które zapewnia, że będzie on funkcjonował w zamierzony i nienaruszalny sposób oraz będzie wolny od nieautoryzowanych manipulacji systemu (zarówno tych umyślnych, jak i przypadkowych).

Natomiast pojęcie **spójności** używane jest najczęściej w odniesieniu do baz danych i może dotyczyć dwóch wymagań. Pierwszym z nich jest zapewnienie, że gromadzone w bazie danych informacje są zgodne ze stanem faktycznym oraz odpowiadają określonemu wycinkowi rzeczywistości. Drugie wymaganie dotyczy zgodności danych przechowywanych w różnych systemach bądź różnych miejscach jednego systemu. Często można spotkać się z taką sytuacją, gdy w celach poprawy wydajności dokonywana jest replikacja bazy danych. Aby uchronić się przed utratą spójności w systemie bazodanowym należy upewnić się, że w prawidłowy sposób działa w nim system obsługi transakcji, który nie dopuści do tego, by w przypadku awarii bądź próby wykonania kilku współbieżnych operacji, baza danych stała się niespójna.

Ostatnim z elementów potrzebnych do zapewnienia bezpieczeństwa informacji jest **dostępność**. Często jest ona niesłusznie lekceważona, jednak odgrywa równie ważną rolę jak dwa poprzednie elementy. Jej rolą jest zapewnienie, że zarówno sprzęt, jak i oprogramowanie systemu informatycznego pracuje w sposób zapewniający dostęp do zasobów uprawnionym do tego użytkownikom. O braku dostępności mówi się wtedy, gdy istnieje taki moment, kiedy użytkownik nie jest w stanie skorzystać z systemu zgodnie z posiadanymi przez niego uprawnieniami. Typowym przykładem systemu, gdzie dostępność odgrywa bardzo ważną rolę jest serwer poczty elektronicznej e-mail. Każdy użytkownik powinien mieć zapewniony ciągły oraz nieprzerwany dostęp do swoich wiadomości oraz do usługi wysyłania poczty. Dostępność powinna być zapewniona nie tylko wobec posiadaczy kont e-mail na danym serwerze, lecz także wobec innych serwerów pocztowych tak, by wszelkie wiadomości przychodzące były przyjmowane prawidłowo.

Zagrożeniem dla dostępności może być zbyt duże obciążenie systemu poprzez uruchomienie zbyt wielu procesów, których system nie jest w stanie obsłużyć. W przypadku publicznie dostępnych systemów webowych istotnym zagrożeniem jest duża liczba zapytań ze strony jednego bądź wielu użytkowników. Istnieją techniki ataku, które przy użyciu dużej liczby zapytań powodują zatrzymanie lub znaczne spowolnienie pracy systemu. System może być niedostępny nie tylko na skutek działania czynników zewnętrznych, ale również na skutek wewnętrznego błędu, nieprawidłowej operacji czy choćby braku zasilania.

Aby chronić system przed utratą tej ważnej cechy, jaką niewątpliwie jest dostępność, stosuje się szereg środków zapobiegawczych. Jako, że dostępność zależy od sprzętu i oprogramowania, konieczne jest używanie zabezpieczeń dla obu tych składowych. Często używanymi zabezpieczeniami dla sprzętu są zasilacze awaryjne czy klimatyzatory, które potrafią zapewnić odpowiednią temperaturę czy wilgotność w pomieszczeniu, w którym znajduje się sprzęt komputerowy. Nieco innymi zabezpieczeniami są algorytmy implementowane bezpośrednio w oprogramowaniu układów cyfrowych. Przykładowo, dyski twarde posiadają mechanizmy, dzięki którym w przypadku awarii sektora może on zostać całkowicie wyłączony z użycia tak, by system, w którym dysk jest zainstalowany, nie tracił cennego czasu próbując odczytać dane z uszkodzonej części dysku. Jeśli chodzi o zabezpieczenia stosowane w oprogramowaniu komputerowym, to należy wspomnieć o różnego rodzaju algorytmach kolejkujących zdarzenia, procesy czy żądania dostępu do zasobów. Algorytmy te najczęściej w czasie rzeczywistym monitorują ruch i nadają zadaniom odpowiednie priorytety po to, by system nie został przeciążony.