Lekcja: Podział zagrożeń dla bazy danych i sposoby przeciwdziałania im.

1. Bazy danych mogą być zagrożone ze strony ataków, bądź też ze strony awarii sprzętowych. Stąd wynika konieczność stosowania zabezpieczeń dla baz danych. Same ataki można podzielić na:
   a) ataki pasywne – sprowadzają się do prowadzenia nasłuchu sieciowego (podglądaniu), gdzie atakujący może śledzić hasło wpisywane na klawiaturze (*np. programy typu keylogger, które rejestrują naciskane klawisze*), nagrać moment wpisywania hasła kamerką, prowadzić nasłuch w sieciach radiowych lub telefonicznych, przechwytywać e-maile oraz pliki, czy w końcu analizować ruch sieciowy (*można przechwytywać dane przesyłane drogą radiową, zapisywać je na dysku i odpowiednim programem np. Aircrack-ng deszyfrować klucz WEP*). Ataki tego typu są trudne do wykrycia.
   b) ataki aktywne – związane są ze zmianą danych w obrębie systemu informatycznego. Atakujący może podszywać się pod inną osobę na podstawie informacji zdobytej poprzez atak pasywny (*np. po rozpoznaniu klucza WEP autoryzuje dostęp swojego komputera do sieci, lub dzięki keyloggerowi zna hasło i loguje się do danych zasobów*), modyfikować komunikaty (*zmieniać oryginalne komunikaty lub je opóźniać*), bądź też blokować usługi poprzez przeciążenia, przeładowania, zagłuszenia, lub fizyczne zniszczenie (*w marcu 2011 roku, 75 – letnia Gruzinka poszukując złomu odcięła część Gruzji i Armenii od Internetu, przecinając łopatą światłowód, myśląc że to przewód z miedzią*)
2. Innymi zagrożeniami mogą być ataki elektromagnetyczne. Tutaj w wyniku generowania pola elektromagnetycznego (*generatory mikrofal, bomby elektromagnetyczne, wybuchy na słońcu*) może dochodzić do uszkodzeń urządzeń elektronicznych oraz danych znajdujących się na nośnikach. Poza tym istnieje pojęcie podsłuchu elektromagnetycznego, gdzie w wyniku promieniowania jakie emitują ekrany komputerowe można je odbierać i odczytywać obraz na innym podsłuchującym urządzeniu (*pierwsze takie urządzenie skonstruował holenderski naukowiec Wim van Eck z Neher Laboratories ok. 10 lat temu, artykuł o tym pojawił się w 2004 r. Trudno jest zbudować takie urządzenie i faktycznie dane przechwycić, ale teoretycznie, przy dużym nakładzie pracy i pieniędzy jest to możliwe*).
3. Bardzo ważnym elementem zabezpieczeń baz danych jest wykonywanie ich kopii zapasowych oraz sposób ich przechowywania. W sytuacji szczególnie ważnych danych powinny one być nie tylko kopiowane, ale też przechowywane w miejscach na tyle odległych geograficznie, aby w przypadku klęsk żywiołowych było możliwe ich odzyskanie.
4. Na podniesienie bezpieczeństwa np. na serwerach wpływać może modyfikacja plików konfiguracyjnych. Do obszarów tych zaliczyć można:
   a) authentication_timeout (integer) – ilość sekund, w czasie których użytkownik powinien zalogować się do systemu, jeżeli czas minie serwer zamyka połączenie
   b) ssl (boolean) – włączenie bezpiecznych połączeń ssl
   c) ssl_renegotiation_limit (integer) – ilość danych przesyłana przez szyfrowanie SSL przed powtórnym negocjowaniem połączenia i wymianą kluczy szyfrujących (*ma*

to zabezpieczać przed złamaniem szyfrowania ssl przez osobę przy dużej ilości zrzutu szyfrowanych danych)

d) ssl_ciphers (string) – selekcja algorytmów szyfrujących, których można użyć w celu zabezpieczenia połączenia