Audyt Bezpieczeństwa stanowisk komputerowych

Cel

1. Zwiększenie poziomu bezpieczeństwa systemów informatycznych sądu.
2. Uświadomienie użytkowników w zakresie znaczenia i konieczności dbania o bezpieczeństwo systemów informatycznych.

Założenia

1. W dobrej praktyce chodzi o kontrolę zabezpieczeń stanowisk i urządzeń komputerowych, jednak nie oznacza to, że sprawdzane jest bezpieczeństwo tylko tych elementów (stanowisk i urządzeń). W rzeczywistości jest to *kontrola bezpieczeństwa całego systemu informatycznego przez pryzmat stanowisk komputerowych*.
2. Szczegółowość kontroli i korzyści, które przyniesie zależą od konstrukcji list audytowych i rzetelności udzielanych odpowiedzi.
3. Aspekt uświadamiania użytkowników jest pochodną przeprowadzanych kontroli.
4. Regularne kontrole i samokontrole zabezpieczenia stanowisk i urządzeń spełniają podstawowe cele szkoleniowe i pozwolą użytkownikom na zapoznanie się m.in. z takimi zagadnieniami jak:
   a. podstawowe pojęcia związane z bezpieczeństwem SI,
   b. podstawowe potrzeby ochrony i cele polityki bezpieczeństwa SI,
   c. następstwa wystąpienia zagrożeń i naruszenia bezpieczeństwa,
   d. funkcjonowanie systemu ochrony,
   e. obowiązki i odpowiedzialność użytkowników SI,
   f. konsekwencje nieautoryzowanego działania (w tym sankcje dyscyplinarne).

Utworzenie narzędzia

1. Lista audytowa – inaczej lista kontrolna (ang. *checklist*) – ma postać zbioru pytań, na które użytkownik odpowiada, najczęściej w sposób binarny: „tak”/„nie”, („jest”/„nie ma”; „spełnione”/„niespełnione”) z zachowaniem możliwości udzielenia odpowiedzi „nie dotyczy”. Czasami w listach audytowych dopuszcza się odpowiedź: „spełnione częściowo”.
2. Zaletą list audytowych jest natychmiastowe *zwrócenie uwagi na występujące problemy*, elementy systemu i zjawiska, które mają znaczenie dla bezpieczeństwa systemu. Co z kolei powinno być punktem wyjścia do podjęcia dalszych działań.
3. Wykorzystanie list do określania poziomu bezpieczeństwa systemu polega na odpowiednim skonstruowaniu *wzorca*, który określa stan idealny i maksymalną liczbę punktów, jaką może uzyskać kontrolowany system. Wzorzec, stanowi więc odniesienie dla uzyskanych wyników.
4. Następnie do poszczególnych pytań przypisuje się liczbę punktów za odpowiedź pozytywną i negatywną (najczęściej „1” za „tak”/„jest”/„spełnione” i 0 za „nie”/„nie ma”/„niespełnione”). Określa się także kolejne poziomy oceny (np. zadowalający, dostateczny, niezadowalający), do których zaliczony będzie system w zależności od liczby uzyskanych punktów.
5. Po udzieleniu odpowiedzi na wszystkie pytania z listy, punkty należy zsumować i wynik porównać ze wzorcem.
6. Wynik może być przedstawiony graficznie, co często ułatwia jego analizę.

Opis funkcjonowania praktyki

1. Dobra praktyka zakłada przeprowadzanie kontroli zabezpieczeń stanowisk i urządzeń komputerowych przy wykorzystaniu metody list audytowych (list kontrolnych).
2. Dane uzyskane podczas kontroli podlegają analizie, co pozwala na wychwycenie słabości systemu i wdrożenie odpowiednich zabezpieczeń.

Korzyści

1. Do korzyści w aspekcie organizacji pracy należy:
   a) zwiększenie bezpieczeństwa systemu informatycznego,
   b) identyfikacja mocnych i słabych stron zabezpieczeń systemu informatycznego,
   c) poprawa funkcjonowania systemu informatycznego,
   d) zwiększenie możliwości kontroli infrastruktury informatycznej,
   e) dostosowanie funkcjonowania i zabezpieczania systemu informatycznego do przepisów prawa i norm ISO,
   f) zmniejszenie liczby sytuacji kryzysowych wynikających z naruszenia bezpieczeństwa systemu informatycznego.
2. Do korzyści w aspekcie pracownika należy:
   a) zwiększenie bezpieczeństwa funkcjonowania stanowiska pracy,
   b) zwiększenie wiedzy na temat zagadnień związanych z bezpieczeństwem SI,
   c) zwiększenie świadomości występowania zagrożeń,
   d) otrzymywanie informacji zwrotnych na temat poziomu zabezpieczeń własnego stanowiska pracy (w tym na temat własnego postępowania wpływającego na bezpieczeństwo systemu),
   e) wykorzystanie potencjału pracowników m.in. w zakresie śledzenia nieprawidłowości działania i występowania incydentów naruszenia bezpieczeństwa informatycznego,
   f) zwiększenie motywacji do przestrzegania zasad bezpieczeństwa podczas korzystania z systemu informatycznego.
3. Do korzyści w aspekcie finansowym należy:
   a) zmniejszenie kosztów związanych z usuwaniem skutków wystąpienia zagrożeń i naruszenia
   b) bezpieczeństwa systemu informatycznego, m.in.:
   - zmniejszenie kosztów braku dostępności systemu,
   - zmniejszenie kosztów napraw,
   - zmniejszenie kosztów odzyskiwania danych.
   c) zmniejszenie kosztów szkoleń, ze względu na wzrost świadomości użytkowników w zakresie bezpieczeństwa systemu informatycznego.

Koszt wdrożenia

Koszty wdrożenia są przede wszystkim *kosztami osobowymi* – kosztami pracy służb informatycznych (głównie na opracowanie list audytowych, narzędzi wspomagających i przeprowadzanie kontroli) oraz kosztami pracy użytkowników poniesionymi na samokontrolę swoich stanowisk i urządzeń:

1. Koszt opracowania i późniejszej aktualizacji list audytowych oraz wzorca oceny poziomu bezpieczeństwa.
2. Koszt analizy wyników kontroli i oceny poziomu bezpieczeństwa.
3. Koszt opracowania informatycznych narzędzi wspomagających przeprowadzanie kontroli, analizowanie wyników i ocenianie poziomu bezpieczeństwa.
4. Koszt przeszkolenia osób odpowiedzialnych za funkcjonowanie praktyki.
5. Koszt przeprowadzania kontroli zabezpieczeń stanowisk i urządzeń komputerowych:
   - przez pracowników oddziału informatyki,
   - przez użytkowników stanowisk i urządzeń.

Inne konieczne nakłady/czynności

Do przeprowadzania kontroli zabezpieczeń stanowisk i urządzeń komputerowych niezbędne jest narzędzie informatyczne wspomagające ten proces, np. formularz internetowy z możliwością zapisywania wyników w bazie.