Eksploatacja i bezpieczeństwo systemów

dr inż. Mirosław Mazurek

Zakład Systemów Złożonych
Bud. F, pok. 305, tel. 17 865 11 04

Bezpieczny system teleinformatyczny

Bezpieczny system komputerowy jest wyidealizowanym urządzeniem, które poprawnie i w całości realizuje tylko i wyłącznie cele zgodne z intencjami właściciela.

Czy istnieje taki system?

W praktyce budowa skomplikowanego systemu spełniającego te założenia jest z reguły niemożliwa.

Powody:

- ryzyko wystąpienia prozaicznych usterek i błędów,

- trudność określenia i sformalizowania często sprzecznych oczekiwań projektanta oprogramowania, programisty, prawowitego właściciela systemu, posiadacza przetwarzanych danych, czy w końcu użytkownika końcowego.

- trudność określenia, że dany program spełnia sformalizowane oczekiwania.

Zarządzanie ryzykiem

Zarządzanie ryzykiem rozumie się jako podejmowanie działań mających na celu**:**

- rozpoznanie,
- ocenę
- sterowanie ryzykiem
- kontrolę podjętych działań.

Celem zarządzania jest ograniczanie ryzyka oraz zabezpieczanie się przed jego skutkami.

- Celem rozpoznania - identyfikacji jest określenie rodzajów ryzyka, które wiążą się z rozważaną inwestycją. Ich prawidłowe rozpoznanie jest o tyle istotne, że umożliwia inwestorowi podjęcie działań mających na celu zabezpieczenie się przed nimi lub ich redukcję.

Zarządzanie ryzykiem

• Oceny ryzyka dokonuje się stosując różne mierniki. Ich wybór zależy od rodzaju ryzyka jakie podlega ocenie. Możliwe jest wskazanie tych czynników ryzyka, na które należy zwrócić szczególną uwagę.

• Sterowanie rozumie się jako podejmowanie działań mających na celu ograniczenie ryzyka do dopuszczalnych rozmiarów.

W sterowaniu ryzykiem wyróżnić można dwa zasadnicze podejścia:

• aktywne - polegające na oddziaływaniu na przyczyny ryzyka

• pasywne - koncentrujące się na zabezpieczaniu przed ewentualnymi stratami.

Zarządzanie ryzykiem

W ramach podejścia aktywnego można podejmować następujące działania:

• **unikanie ryzyka** - wiąże się z zaniechaniem inwestycji, gdy jest ona obarczona zbyt dużym ryzykiem.

• **działania prewencyjne** - mają na celu zapobieganie zdarzeniom losowym.

• **przenoszenie ryzyka na inne podmioty** - wiąże się z transferem odpowiedzialności za pokrycie ewentualnych strat. Może ono przyjmować takie formy, jak np.: ubezpieczenia, gwarancje, poręczenia, transakcje terminowe.

• **dywersyfikacja -** ma na celu zmniejszenie poziomu ryzyka przez inwestowanie w różne działalności, których stopy zwrotu są mniej niż absolutnie dodatnio skorelowane. Utworzenie dobrze zdywersyfikowanego portfela projektów inwestycyjnych spowodować może znaczne,
a nawet całkowite zredukowanie ryzyka specyficznego.

Zarządzanie ryzykiem

Zapewnianie bezpieczeństwa sprowadza się najczęściej do całościowego zarządzania ryzykiem:

- określane są potencjalne zagrożenia,

- szacowane prawdopodobieństwo ich wystąpienia,

- oceniany potencjał strat

- podejmowanie kroków zapobiegawczych w zakresie, który jest racjonalny z uwagi na możliwości techniczne i względy ekonomiczne.

Polityka bezpieczeństwa

Polityka bezpieczeństwa informacji jest zbiorem spójnych, precyzyjnych reguł i procedur, według których dana organizacja buduje, zarządza oraz udostępnia zasoby i systemy informacyjne i informatyczne. Określa ona, które zasoby i w jaki sposób mają być chronione.

Polityka powinna obejmować wskazanie możliwych rodzajów naruszenia bezpieczeństwa (jak np. utrata danych, nieautoryzowany dostęp), scenariusze postępowania w takich sytuacjach i działania, które pozwolą uniknąć powtórzenia się danego incydentu. Polityka bezpieczeństwa definiuje ponadto poprawne i niepoprawne korzystanie z zasobów (np. kont użytkowników, danych, oprogramowania).

Istotne jest, aby polityka bezpieczeństwa była dokumentem spisanym i znanym oraz zrozumianym przez pracowników organizacji korzystających z zasobów informatycznych. Dotyczy to także klientów organizacji (użytkowników jej zasobów).

Polityka bezpieczeństwa

Polityka powinna odnosić się do następujących zagadnień:

- co podlega ochronie?
  - informacja (dane)
  - systemy teleinformatyczne (sprzęt)
- jak chronimy krytyczne zasoby?

Projektując mechanizmy ochrony informacji należy określić następujące elementy:

- model bezpieczeństwa
- mechanizmy kontroli dostępu
- poziomy uprawnień (jakie poziomy uprawnień istnieją i jakie są zasady ich przyznawania)
- mechanizmy identyfikacji i zapewnienie autentyczności (na poziomie fizycznym i systemów)
- śledzenie zdarzeń w systemie (jakie mechanizmy /programy/ procedury stosowane są do śledzenia zmian w systemach)

Normy dotyczące bezpieczeństwa informacji

PN-I-13335-1: 1999
„Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych”

ISO/IEC TR 13335-2:2003
„Zarządzanie i planowanie bezpieczeństwa systemów informatycznych”

ISO/IEC TR 13335-3:2003
„Techniki zarządzania bezpieczeństwem systemów informatycznych”

PN ISO/IEC 17799:2003
„Praktyczne zasady zarządzania bezpieczeństwem informacji”

PN –I- 07799-2:2005
„Systemy zarządzania bezpieczeństwem informacji – Specyfikacja i wytyczne stosowania” (przyjęta do ustanowienia we wrześniu 2004; identyczna z BS 7799-2:2002)

Miary poziomu bezpieczeństwa

Bezpieczeństwo teleinformatyczne oznacza poziom uzasadnionego (np. analizą ryzyka) zaufania, że potencjalne straty wynikające z niepożądanego (przypadkowego lub świadomego) ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej i przesyłanej za pomocą systemów teleinformatycznych nie zostaną poniesione.

Wzór pozwalający na wyliczenie bezwzględnej wagi błędu na podstawie jego cech systematycznych definiuje się jako CVSS (Common Vulnerability Scoring System).

Miara podstawowa (Base CVSS) wynikająca z tych cech błędu, które są wspólne dla wszystkich podatnych implementacji i niezmiennych w czasie (np. możliwość zdalnego wykorzystania błędu, brak konieczności uwierzytelnienia).

Miara zmienna w czasie (Temporal CVSS) biorąca pod uwagę czynniki powstające po publikacji informacji o błędzie.

Miara środowiskowa (Environmental CVSS) uwzględniająca lokalną specyfikę w konkretnym systemie teleinformatycznym. Miara ta jest ustalana indywidualnie przez każdą organizację.

Błędy zabezpieczeń

- Błędy implementacyjne

Definiowane jako wszelkie pomyłki techniczne popełniane przez programistów na skutek ich niewiedzy lub nieuwagi.

Przykłady błędów:

- niewystarczające sprawdzanie parametrów lub wyników działania wywołań systemowych (może prowadzić do podatności na ataki typu przepełnienie bufora, nadużycie szablonu formatowania funkcji *printf() (ang. format string attack) czy przekroczenie zakresu liczb całkowitych)

- możliwość przejęcia pełnej kontroli nad procesem przez osoby niepowołane oraz możliwość bezpośredniej interakcji z systemem operacyjnym.

Błędy zabezpieczeń

- Błędy projektowe

sytuacja, w których założenia dla oprogramowania opierały się na błędnych przesłankach, np. na mylnym rozumieniu zasad funkcjonowania sieci komputerowych i budowy wykorzystywanych protokołów komunikacyjnych.

Przykłady błędów:

- wykorzystanie szyfrów podatnych na ataki, (protokół Needhama-Schroedera – Kerberos),

- nieprawidłowy dobór mechanizmów uwierzytelniania,

- pełne zaufanie informacjom przesyłanym przez klienta w architekturze klient-serwer (Ich skutkiem może być sytuacja, w której nie można ufać wynikom pracy aplikacji i integralności przetwarzanych przez nią danych).

Błędy zabezpieczeń

- Błędy konfiguracyjne

definiowane jako pomyłki popełniane przez administratorów, którzy przygotowują oprogramowanie do wykorzystania przez użytkowników.

Mogą one powstawać na skutek niezrozumienia dokumentacji lub sposobu działania aplikacji, albo zwykłej niestaranności.

Przykłady błędów:

- ustawienie trywialnych haseł dla uprzywilejowanych kont,

- udostępnienie zbędnej funkcjonalności bez adekwatnej kontroli dostępu.

Błędy zabezpieczeń

- Błędy operatora

zachowania użytkowników, którzy nie rozumieją w pełni funkcji oprogramowania i zasad działania systemów komputerowych.

Przykłady błędów:

- uruchamianie załączników od niepewnych nadawców przysłanych w poczcie elektronicznej,

- ignorowanie komunikatów ostrzegawczych,

- przypadkowa zmiana opcji programu,

- utrata nośnika z kopią zapasową danych.

Sposoby walki z zagrożeniami bezpieczeństwa

- **skuteczne zapobieganie powstawaniu usterek**

- **budowanie systemów w sposób, który ogranicza ewentualne problemy wynikające z naruszenia zabezpieczeń lub niepożądanej aktywności uprawnionego użytkownika**

- **zredukowanie ryzyka pomyłek przy tworzeniu oprogramowania**

    - Odpowiednia budowa protokołów i interfejsów

    - Wybór metod programistycznych

    - Testowanie jakości aplikacji
        - Przegląd kodu źródłowego
        - Testy typu czarna skrzynka
        - Testy siłowe

Testowanie jakości aplikacji

- Przegląd kodu źródłowego (inspekcja kodu w poszukiwaniu potencjalnie niebezpiecznych konstrukcji lub oczywistych pomyłek; statyczna analiza kodu - zaletą jest wysoka skuteczność, wadą natomiast pozostaje wysoki koszt zatrudnienia eksperta oraz czasochłonność procesu)

- Testy typu czarna skrzynka (badania zachowania programu binarnego lub platformy, bez dodatkowej wiedzy o sposobie wewnętrznej konstrukcji programu (użycie ang. Debuggerów lub skanerów zabezpieczeń (Nmap, Nessus, WebInspect, itp). Zaletą jest możliwość zlecenia takich badań osobie trzeciej bez konieczności przekazania jej kodu źródłowego. Wadą jest trudność w diagnozowaniu subtelnych problemów implementacyjnych.

- Testy siłowe (działania przeprowadzane za pomocą narzędzi zautomatyzowanego losowego testowania (ang. fuzzing), polegające na generacji przypadkowych danych wejściowych i obserwowaniu zachowania programu. Zaletą jest pełna automatyzacja procesu i możliwość ujawnienia bardzo złożonych błędów, np. wynikających z interakcji z systemem operacyjnym. Ich wadą jest niekompatybilność z bardziej skomplikowanymi protokołami komunikacyjnymi (co może prowadzić do odrzucenia wszelkich losowo wygenerowanych sekwencji na bardzo wczesnym etapie obróbki danych przez program).

Audyt - podstawowe definicje

Audyt to ocena osoby, projektu, produktu, organizacji bądź systemu.

Jako główny cel audytu uznaje się wyrażenie opinii na temat osoby, organizacji systemu itd. w oparciu o przeprowadzone badania i testy.

Ze względów praktycznych celem audytu jest dostarczenie informacji że w badanym przedmiocie nie ma istotnych błędów. Audyt wykonują kompetentne i niezależne zespoły które jasno określają czy dany przedmiot audytu spełnia stawiane mu wygania. Obecnie w każdej dziedzinie ludzkiego życia występują audyty. Są to np.:

- audyt informatyczny
- audyt finansowy
- audyt jakości
- audyt etyczny
- audyt oprogramowania
- audyt personalny
- audyt systemu
- audyt wiedzy

Podstawowe definicje

- Audyt IT to działanie mające na celu zebranie i ocena dowodów określających czy system informatyczny a także jego zasoby spełniają stawiane mu cele. Najczęściej sprawdza się czy system utrzymuje integralność danych, dostarcza prawidłowych informacji, jest efektywny a także czy prawidłowo wykorzystuje podległe mu zasoby. Podczas audytu sprawdza się również czy system wystarczająco chroni się przed niepożądanymi zdarzeniami i czy jest bezpieczny.

- Występuje wiele standardów którymi kieruje się podczas wykonywania audytu IT. Najpopularniejsze to: ISO 900, COBIT,ITIL, ISO/IEC 27001 bądź ISO/IEC 27002

ISO 9001

- ISO 9001 - normę tę mogą stosować wszystkie organizacje, niezależnie od ich wielkości i rodzaju. Ukierunkowana jest ona na zrozumienie i spełnienie wymagań klienta, a więc określonych potrzeb względem wyrobów danej organizacji, przyjęcie podejścia procesowego, dostarczanie wyników skuteczności procesów oraz ich ciągłe doskonalenie w oparciu o obiektywne pomiary. Standard ten zaleca objęcie procesów organizacji cyklem PDCA, znanym również jako Cykl Deminga.

- Do głównych wymagań normy ISO 9001 należą m.in.: wprowadzenie nadzoru nad dokumentacją i zapisami, zaangażowanie kierownictwa w budowanie systemu zarządzania jakością, usystematyzowanie zarządzania zasobami, ustanowienie procesów realizacji wyrobu, dokonywanie systematycznych pomiarów (zadowolenia klienta, wyrobów, procesów).

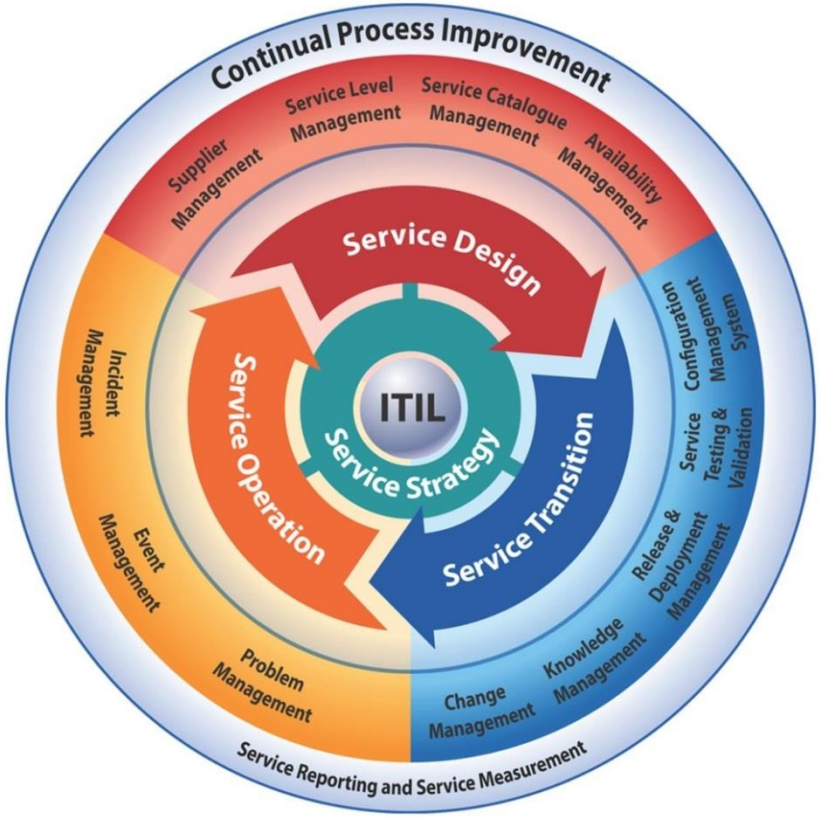
COBIT

- COBIT to standard opracowany przez ISACA oraz IT Governance Institue który zawiera zbiór praktyk z zakresu IT które są wykorzystywane przez audytorów badających bezpieczeństwo systemów informatycznych.
- Standard ten pomaga organizacjom osiągać optymalną wartość z technologii informatycznych, ponieważ wskazuje jak zachować równowagę pomiędzy uzyskiwaniem korzyści a optymalizacją poziomów ryzyka oraz wykorzystywania zasobów. Umożliwia całościowy nadzór i zarządzanie nad informacjami i odpowiednimi technologiami w organizacji, obejmując wszystkie biznesowe oraz funkcjonalne obszary odpowiedzialności, mając na uwadze związane z IT oczekiwania interesariuszy wewnętrznych i zewnętrznych.
- Standardy COBIT są uniwersalne i przydatne dla organizacji różnej wielkości, firm komercyjnych, podmiotów sektora publicznego czy organizacji non-profit.

Podstawowe definicje

- ITIL to kodeks postępowania dla IT. Zawiera zbiór zaleceń w jaki sposób efektywnie i skutecznie oferować usługi informatyczne. Początki ITIL sięgają połowę lat 80 XX wieku. Pierwsza książka zawierająca zalecenia nosi nazwę HelpDesk i ukazała się w 1989r. Po 22 latach wydano drugą wersję a w 2007 trzecią. Ostatnia wersja z 2007 zawiera 5 opracowań :

- Service Startegy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement



ISO/IEC 27001

- ISO/IEC 27001 to międzynarodowa norma zawierająca standardy zarządzania bezpieczeństwem informacji. Polski odpowiednik to PN-ISO/IEC 27001 Norma ta jest specyfikacją systemów zarządzania bezpieczeństwem informacji na zgodność z którą są prowadzone audyty zakończone wydaniem certyfikatu. W normie tej wyróżnia się 11 obszarów które mają wpływ na bezpieczeństwo informacji przesyłanych w organizacji:

- Polityka bezpieczeństwa, Organizacja bezpieczeństwa informacji, Zarządzanie aktywami, Bezpieczeństwo zasobów ludzkich, Bezpieczeństwo fizyczne i środowiskowe, Zarządzanie systemami i sieciami, Kontrola dostępu, Zarządzanie ciągłością działania, Pozyskiwanie, rozwój i utrzymanie systemów informatycznych, Zarządzanie incydentami związanymi z bezpieczeństwem informacji, Zgodność z wymaganiami prawnymi i własnymi standardami.

Certyfikat CISA

- CISA to certyfikat związany z bezpieczeństwem sieci komputerowych. W chwili obecnej egzamin CISA (wydawany przez międzynarodową organizację ISACA) można zdawać w około 60 państwach na świecie. W Polsce jest to możliwe w Warszawie 2 razy w roku: czerwiec oraz grudzień. Egzamin składa się z 200 pytań testowych o wysokim poziomie trudności. Osoby przystępujące do egzaminu sprawdzane są z:

- Powszechnie znanych standardów wymogów oraz praktyk audytu systemów informatycznych
- Zabezpieczeń kontroli poprawności danych, planowania ciągłości działania oraz procesów testowania
- Procesów informatycznych infrastruktury sieciowej i telekomunikacyjnej
- Praktyk administrowania oraz wykorzystywania zasobów
- Utrzymywania oraz rozwoju systemów informatycznych.

Podstawowe elementy audytu IT

- Podczas audytu IT najczęściej sprawdza się architekturę sieci, system backupowy, zabezpieczenia antywirusowe, poszczególne stacje robocze.

- W przypadku stacji roboczych sprawdza się: legalność zainstalowanego oprogramowania, sprawdzenie jakie uprawnienia posiada danych użytkownik na stacji a także łatwość dostępu do urządzenia przez nieuprawnione osoby (np. firma sprzątająca, przypadkowe osoby).

- Ważnym elementem jest także sprawdzenie zabezpieczeń antywirusowych, oraz firewall. Istotnym elementem są aktualne bazy wirusów a także aktywne zapory sieciowe.

Podstawowe elementy audytu IT

- W przypadku systemu backupowego sprawdza się czy kopie wykonywane są wg ustalonego harmonogramu a także sam harmonogram - czy jest adekwatny do danych które są przechowywane w systemie. Istotnym elementem kontroli jest sprawdzenie jak przechowywane są nośniki wykorzystywane do backupu. Dodatkowo zleca się testowe odzyskanie danych z wykorzystaniem wcześniej wykonanego backupu.

- Ważnym elementem do sprawdzenia są punkty dystrybucyjne (serwerownie). Sprawdza się kontrolę dostępu , wyposażenie pomieszczenia (szafy teleinformatyczne, czujniki temperatury, klimatyzacja), zasilanie awaryjne , legalność używanego oprogramowania oraz konfigurację urządzeń.

Podstawowe elementy audytu IT

- Bardziej złożona jest kontrola architektury sieci ponieważ w niej zawiera się: poprawne wykorzystywanie zdalnego dostępu do zasobów firmy przez pracowników, ograniczenie dostępu z Internetu do usług które są wymagane, odseparowanie od siebie siedzi w poszczególnych działach tak aby informacje były udostępniane tylko tym osobom które wykonują na nich prace a także weryfikacja czy Administrator posiada schemat całej sieci.

- W przypadku takiego audytu ważne jest sprawdzenie polityki bezpieczeństwa (jej jakości i to czy faktycznie taki dokument został stworzony). W jeszcze wielu firmach i instytucjach taki dokument nie został stworzony przez co użytkownicy są destrukcyjni dla działania firmy.

Audyt wykonywany przez firmy

- Audyt informatyczny wykonywany przez firmy jest zespołem czynności prowadzących do uzyskania i oceny informacji na temat zasobów sprzętowych, aktualnie zainstalowanego oprogramowania oraz ważnych licencji na programy. Wykonuje się go w celu zapewnienia, że firma działa na całkowicie legalnym oprogramowaniu, sprzęt jest wykorzystywany efektywnie i zgodnie z przeznaczeniem a poufne informacje dostatecznie zabezpieczone przed nieautoryzowanym dostępem. Informacje te pozwalają zaplanować zakupy sprzętu i licencji oraz precyzyjniej reagować w sytuacjach kryzysowych. Audyty informatyczne można podzielić ze względu na podmiot działania - sferę, która jest kontrolowana.

- Kontrola może być przeprowadzona przez pracowników firmy (audyt wewnętrzny), znacznie częściej jednak występuje audyt zewnętrzny, zlecony wyspecjalizowanej firmie. Ta druga opcja pozwala uzyskać bardziej obiektywne dane.

Strefy audytu

- Audyt bezpieczeństwa teleinformatycznego - audyt jest przeprowadzany przez Certyfikowanych inżynierów systemów Red Hat i Microsoft oraz certyfikowanych trenerów szkoleń firmy Microsoft

- Audyt legalności przetwarzania danych osobowych - polega na weryfikacji istniejącego stanu zabezpieczeń przetwarzanych danych

- Audyt oprogramowania i legalności oprogramowania – jest to ocena organizacji jednostki audytowanej pod względem zarządzania produktami informatyki jakimi są programy komputerowe

- Audyt sprzętu i infrastruktury IT - chcąc dobrze gospodarować sprzętem komputerowym i siecią teleinformatyczną funkcjonującą w firmie, należy przygotować kompletną bazę zawierającą wszystkie dane urządzeń w niej działających i ich możliwości

Zakres prac

- Zapoznanie się z infrastrukturą LAN, WAN
- Zapoznanie się z zabezpieczeniami i dostępem do Internetu
- Zapoznanie się z infrastrukturą serwerową
- Zapoznanie się ze strukturą katalogową, strukturą plikową
- Zapoznanie się z pracującym rozwiązaniem antywirusowym
- Zapoznanie się z pracującym systemem do backupu
- Zapoznanie się z sytuacją dotyczącą licencjonowania produktów posiadanych przez Klienta
- Zapoznanie się z systemami biznesowymi pracującymi u klienta
- Analiza pracy systemu pocztowego
- Analiza pracy stacji roboczych, ich funkcji i stanu
- Wstępna analiza potrzeb użytkowników systemu informatycznego

Korzyści wynikające z audytu

- Fachowa ocena poziomu bezpieczeństwa teleinformatycznego
- Wykrycie słabych punktów w systemie zabezpieczeń wraz z oceną potencjalnych zagrożeń
- Wiarygodność dla kontrahentów
- Opracowanie polityki bezpieczeństwa i wdrożenie jej do systemu
- Usprawnienie działania sieci teleinformatycznej i zarządzania nią
- Dostarczenie narzędzi oraz środków do przeciwdziałania zagrożeniom
- Zmniejszenie ryzyka związanego z ujawnieniem danych przechowywanych w systemie
- Personel zna zasady bezpieczeństwa teleinformatycznego

Przykładowe działania podczas audytu

- Skanowanie szczelności zabezpieczeń antywirusowych
- Sprawdzenie bezpieczeństwa serwera www
- Testy systemu obsługi poczty
- Analiza bezpieczeństwa DNS
- Analiza systemu firewall
- Testy penetracyjne
- Uwierzytelnienie haseł użytkowników
- Sprawdzenie innych elementów systemu informatycznego firmy
- Ocena zagrożeń i przedstawienie konkretnych możliwości na rozwiązanie istniejących problemów oraz działań prewencyjnych, mających zapobiec ich występowaniu w przyszłości

Kto może wykonać audyt?

- IT AUDITOR
- Versoft
- BGP
- Lizard
- CompNet
- NeoLogic

- Ceny takich audytów określane są indywidualnie dla każdego klienta, ponieważ należy określić zakres i strefy audytu oraz wziąć pod uwagę wielkość danej firmy która zleca taki audyt.

W końcowym raporcie zawarte są również takie informacje jak:

- Informacje dotyczące Audytorów oraz daty przeprowadzenia audytu
- Wyszczególnienie testów, jakie zostały wykonane (np. założenia testu, wykonanie testu, przebieg testu, wnioski i sugestie zabezpieczeń)
- Podsumowanie audytu
- Zalecenia i rekomendacje

Raporty kończą się zazwyczaj podsumowaniem zabezpieczeń gdzie poddawany jest ocenie ogólny stan zabezpieczeń infrastruktury teleinformatycznej oraz wskazane punkty, które powinny zostać poprawione.