„Wybawi się od niebezpieczeństwa jedynie ten, kto czuwa
także gdy czuje się bezpieczny”

Publiusz Siro

Audyt bezpieczeństwa

BERNADETTA
STACHURA – TERLECKA

Definicja

Audyt – systematyczna i niezależna ocena danej organizacji, systemu, procesu, projektu lub produktu.

BERNADETTA
STACHURA – TERLECKA

Podział

Audyt dzielimy ze względu na osobę wykonującą:

- Wewnętrzny,
- Zewnętrzny.

Typy audytu:

- audyt działalności
- audyt ekologiczny
- audyt energetyczny
- audyt etyczny
- audyt finansowy
- audyt informatyczny
- audyt jakości
- audyt marketingowy
- audyt operacyjny
- audyt oprogramowania
- audyt personalny
- audyt systemu
- audyt wiedzy
- audyt zgodności
- audyt bezpieczeństwa

BERNADETTA
STACHURA – TERLECKA

Definicja

Audyt bezpieczeństwa - niezależny przegląd i sprawdzenie zapisów oraz funkcji systemu przetwarzania danych w celu sprawdzenia prawidłowości kontroli systemowej zapewnienie zgodności z przyjętą polityką bezpieczeństwa i procedurami działania wykrycia przełamań bezpieczeństwa oraz w celu zalecenia określonych zmian w kontroli, w polityce bezpieczeństwa i w procedurach.[1]

[1] PN-I-2000:2002

BERNADETTA
STACHURA – TERLECKA

Cele przeprowadzania audytu bezpieczeństwa

Głównym celem przeprowadzania audytu bezpieczeństwa jest znalezienie błędów w funkcjonowaniu systemu kontroli, uprawnień użytkowników, zabezpieczeń oraz wykorzystanie analizy ryzyka do oceny które z zaistniałych nieprawidłowości są najważniejsze i wymagają dokładnej oceny.

BERNADETTA
STACHURA – TERLECKA

Fazy audytu bezpieczeństwa

Audyt składa się z 5 faz, które następują po określeniu tematu audytu, jego celów oraz zakresu:

Faza 1 – Planowanie:

- Określanie potrzebnych zasobów ludzkich i materialnych potrzebnych do przeprowadzenia audytu,
- Identyfikacja źródeł informacyjnych – polityki, procedur, logów,
- Wskazanie lokalizacji obiektów objętych audytem.

Faza 2 – Procedury audytowe i etapy gromadzenia informacji:

- Identyfikacja i wybór elementu (systemu) do przeprowadzenia kontroli,
- Wskazanie osób do przeprowadzenia wywiadu,
- Identyfikacja i pozyskanie potrzebnych polityk oraz standardów,
- Opracowanie procedur audytowych do przeprowadzenia weryfikacji i testów kontrolnych.

Faza 3 – Procedury do oceny wyników testów lub przeglądu:

- Identyfikacja elementu objętego przeglądem i ocena wyników audytu.

Faza 4 – Procedury prowadzenia rozmów z kierownictwem:

- Określenie procedur dotyczących przedstawienia raportów kierownictwu,
- Opracowanie procedur dotyczących komunikowania się w trakcie działań audytowych.

BERNADETTA
STACHURA – TERLECKA

Fazy audytu bezpieczeństwa

Faza 5 – Opracowanie raportu:

- Identyfikacja działań poaudytowych,
- Identyfikacja procedur dotyczących testów mechanizmów kontrolnych,
- Przegląd i ocena znaczących dokumentów, polityk i procedur.

BERNADETTA
STACHURA – TERLECKA

Dokumentacja

Dokumentacja audytu powinna zawierać:

- Zakres i cel audytu,
- Program audytu,
- Kolejne kroki jakie zostały wykonane w ramach przeglądu,
- Zgromadzone dowody,
- Wnioski z przeprowadzonego audytu,
- Rekomendacje modyfikacji konfiguracji systemów oraz procedur,
- Opracowane raporty,
- Przegląd działań audytora dokonywanych przez kierownictwo,
- Metodę rozwiązania problemów,
- Instrukcje zapewniające podniesienie poziomu bezpieczeństwa przedmiotu audytu.

BERNADETTA
STACHURA – TERLECKA

Co podlega audytowi bezpieczeństwa

Audytowi bezpieczeństwa teleinformatycznego podlegają przede wszystkim:

- Możliwość nieautoryzowanego dostępu do danych i nieautoryzowanego ich przetwarzania,
- Dostępność i ciągłość działania,
- Zabezpieczenia przeglądarek internetowych,
- Poziom patchy systemu operacyjnego,
- Konfiguracja modemu / routeru,
- Zabezpieczenia systemu plików,
- Uprawnienia użytkowników,
- Uprawnienia grup,
- Zabezpieczenia serwerów pocztowych,
- Parametry wykorzystywanych protokołów,
- Obecność tylnych wejść ('backdoors'),
- Dostęp do usługi FTP,
- Zabezpieczenia systemu NFS,
- Możliwość ataku wykorzystującego przepełnienie bufora,
- Ustawienia crontab,
- Zabezpieczenia systemu haseł,
- Odporność na ataki stosujące inżynierię społeczną.

BERNADETTA
STACHURA – TERLECKA

Prawa i obowiązki audytora

Statut audytu		
Obowiązki	**Uprawnienia**	**Odpowiedzialność**
• Plany i cele • Zakres (działania) • Zadania • Niezależność • Relacje wzajemne z audytem zewnętrznym • Wymagania stron audytowych	• Analiza ryzyka • Prawo dostępu do informacji, personelu, pomieszczeń oraz systemów potrzebnych do przeprowadzenia audytu • Struktura organizacyjna	• Ścieżka raportowania do wyższego kierownictwa • Ocena realizacji zadań • Ocena personelu • Ocena zgodności ze standardami • Ocena audytu wykonywania planu audytu • Uzgodnione działania (np. kary w przypadku niewykonania obowiązków którejś ze stron)

BERNADETTA STACHURA – TERLECKA

Normy

Numer	Nazwa
PN-I-13335-1:1999	Technika informatyczna, Wytyczne do zarządzania bezpieczeństwem systemów informatycznych Pojęcia i modele bezpieczeństwa systemów informatycznych
PN-ISO/IEC 17799:2007	Technika informatyczna, Techniki bezpieczeństwa, Praktyczne zasady zarządzania bezpieczeństwem informacji
PN-ISO/IEC 27001:2007	Technika informatyczna, Techniki bezpieczeństwa, Systemy zarządzania bezpieczeństwem informacji, Wymagania
PN-ISO/IEC 27005:2010	Technika informatyczna, Techniki bezpieczeństwa, Zarządzanie ryzykiem w bezpieczeństwie informacji
PN-ISO/IEC 27006:2009	Technika informatyczna, Techniki bezpieczeństwa, Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji
PN-ISO/IEC 27000:2012	Technika informatyczna, Techniki bezpieczeństwa, Systemy zarządzania bezpieczeństwem informacji, Przegląd i terminologia
PN-EN ISO 27799:2010	Informatyka w ochronie zdrowia, Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002

BERNADETTA
STACHURA – TERLECKA

Etyka zawodowa

Członkowie stowarzyszenia CISA oraz CISM powinni:

1. Wspomagać wdrażanie właściwych standardów, procedur i mechanizmów kontrolnych systemów informatycznych oraz wspierać działania mające na celu zachowanie zgodności z nimi.
2. Służyć pilnie, lojalnie i uczciwie, w interesie właściwych stron oraz nie uczestniczyć świadomie w żadnych nielegalnych lub niewłaściwych działaniach.
3. Zachowywać prywatność i poufność informacji pozyskanych w czasie pełnienia obowiązków, chyba, że ujawnienie wymagane jest przez prawo. Informacje te nie mogą być używane w celu osiągnięciu własnych korzyści ani wydawane niewłaściwym stronom.
4. Wypełniać swoje obowiązki w sposób niezależny i obiektywny i unikać działań grożących utratą niezależności lub obiektywności, lub mogących do niej prowadzić.
5. Zachowywać kompetentność w obszarach związanych z audytem i kontrolą systemów informatycznych.
6. Wyrażać zgodę na podejmowanie tylko takich działań, które całkowicie będą mogły być przeprowadzone w ramach zawodowych kompetencji.

BERNADETTA
STACHURA – TERLECKA

7. Wypełniać swoje obowiązki z należytą starannością.
8. O rezultatach wykonanych audytów i (lub) prac kontrolnych informować odpowiednie strony, ujawniając wszystkie poznane istotne fakty, które, jeśli nie zostałyby ujawnione, mogłyby zafałszować raporty dotyczące operacji lub ukryć niezgodne z prawem praktyki.
9. Wesprzeć działania edukacyjne kierowane do użytkowników, środowiska zawodowego, społeczności szeroko rozumianych odbiorców, kadr kierowniczych, zarządów, w celu poszerzenia ich rozumienia audytu i kontroli systemów informatycznych.
10. Utrzymywać wysokie standardy zachowania i charakteru i nie angażować się w działania dyskredytujące dla zawodu.

BERNADETTA
STACHURA – TERLECKA

Dziękuję za uwagę

BERNADETTA
STACHURA – TERLECKA