POZNAŃSKIE
CENTRUM
SUPERKOMPUTEROWO
SIECIOWE

Problemy bezpieczeństwa IT w projekcie „e-podręczniki”

Poznań, 06-03-2013

POZNAŃSKIE
CENTRUM
SUPERKOMPUTEROWO
SIECIOWE

Najważniejsze problemy bezpieczeństwa w projekcie „ePodręczniki”

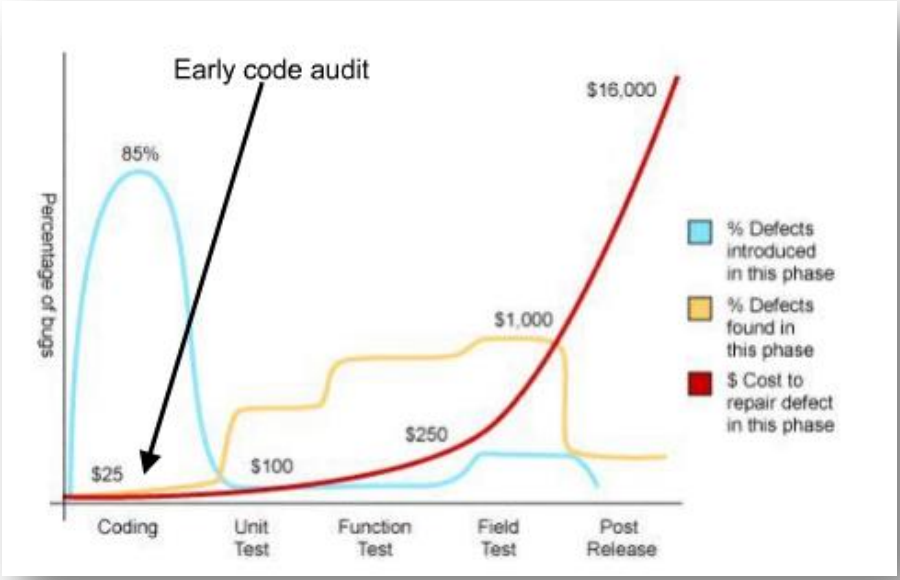
- Specyficzne dla projektu
  - Wiele technologii i kanałów dostępowych
  - Możliwy DoS w wyniku normalnego użytkowania
  - Tysiące „testerów”
  - Bardzo wczesny *release*
  - Duże znaczenie kwestii PR
- Ogólne
  - Błędy na poziomie projektu
  - Nieodpowiednia konfiguracja środowiska na wszystkich warstwach
  - Luki bezpieczeństwa w oprogramowaniu
  - Nieodpowiednie lub źle użyte systemy bezpieczeństwa

Kompleksowa ochrona

- Bezpieczeństwo nie może być cechą dodaną po zakończeniu projektu (to za drogo kosztuje)

Przykład: błędy oprogramowania. Naprawianie ich po wydaniu aplikacji może być kilkaset razy droższe niż na etapie pisania kodu!

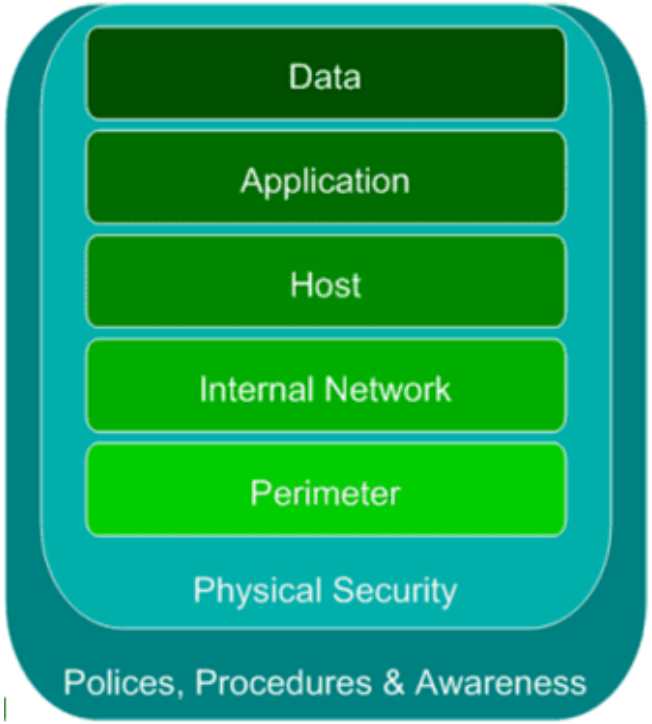
Marco M. Morana - 2006



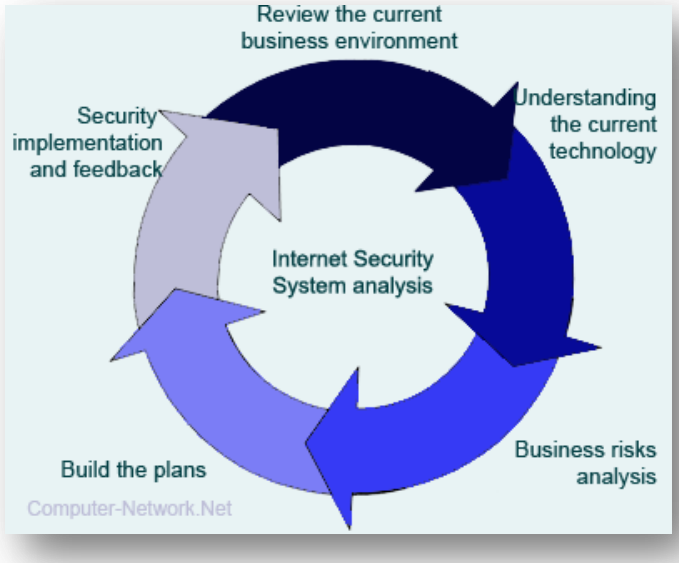
Źródło: *Building Security Into The Software Life Cycle,* Marco M. Morana, 2006

Strategia Defense-in-Depth

- Ochrona dogłębna – na wielu różnych warstwach
  - Napastnik znajdzie błąd np. w aplikacji WWW, ale nie wykorzysta go, gdy:
    1. Serwer WWW jest dobrze skonfigurowany. Nie można wykonać w zaatakowanym systemie dowolnego kodu.
    2. System IDS wykryje niepożądane działania i powiadomi administratora.
  - Strategia podwyższa koszt udanego ataku, czyniąc go nieopłacalnym dla napastnika



Bezpieczeństwo jako proces



- Ocena bezpieczeństwa jest ważna tylko dla określonego stanu
- Zmienia się:
  - Stan wiedzy w zakresie bezpieczeństwa IT
  - Analizowane środowisko (dodatkowe aplikacje, nowe serwery, więcej kont użytkowników, inny administrator…)

Podstawowe działania w zakresie bezpieczeństwa

- Audyty koncepcji rozwiązań sprzętowych i programowych
- Szkolenia z zakresu bezpiecznego programowania
- Doradztwo i ekspertyzy w zakresie konfiguracji rozwiązań oraz technologii
- Audyty kodu tworzonych aplikacji
- Przeglądy konfiguracji systemów
- Testy penetracyjne gotowej infrastruktury
- Monitoring i analiza ruchu sieciowego oraz reagowanie na incydenty
- Wsparcie dla kwestii prawnych (UoODO)

Kontakt

- **Gerard Frankowski**, Zespół Bezpieczeństwa PCSS
  - gerard.frankowski@man.poznan.pl
- Marcin Jerzak, Zespół Bezpieczeństwa PCSS
  - marcin.jerzak@man.poznan.pl

POZNAŃ SUPERCOMPUTING AND NETWORKING CENTER

Dziękuję za uwagę!

Poznań Supercomputing and Networking Center
affiliated to the Institute of Bioorganic Chemistry of the Polish Academy of Sciences,
ul. Noskowskiego 12/14, 61-704 Poznań, POLAND,
Office: phone center: (+48 61) 858-20-00,
fax: (+48 61) 852-59-54,
e-mail: office@man.poznan.pl, http://www.man.poznan.pl