Praktické zkušenosti s bezpečností frontendu z pohledu projektového managementu

Petr Pinkas

SOCIETE
GENERALE
GROUP

KB

Agenda

- Představení
- Historie
- Bezpečnost v projektovém řízení
- Riziko vs. náklad
- Eliminace rizik
- Spolupráce s uživatelem
- Řešení chyb v produkčním prostředí
- Další kroky v řešení bezpečnosti

Představení

- **Petr Pinkas**
  - 2010 – Head of PM Operations
  - 2009 – Head of PM Development
  - 2007-2009 PMM Process engineer
  - 2002-2007 Head of DCS CC
  - 2001-2002 Integration manager
  - 2000-2001 WebMaster KB
  - 1996-2000 UVT

Historie

- **rok 2000**
  - bezpečnost řešena pouze na úrovni IT, minimální participace businessu
  - bezpečnost řešena pouze technickými prostředky
  - KB a.s. implementace PKI
  - minimální investice
- **rok 2007**
  - první vlna útoků na české banky
  - vir Sinoval (zcizení autentizačních prostředků)
  - spolupráce mezi bankovními domy a antivirovými firmami
- **rok 2007**
  - one time password v aplikaci MB – implementace za 2 měsíce od prvního útoku
- **rok 2008**
  - Fraud Detection System
- **rok 2009**
  - bezpečnost je řešena na všech úrovních (IT, BU, PM)
  - bezpečnost je nedílnou součástí jak projektových procesů, tak aplikací

- **IF (Idea Formulation)**
  - reálnost návrhu vzhledem ke globální koncepci
  - constrains
- **PD (Project Definition)**
  - spolupráce se security konrespondentem
    - validace
    - architektonický návrh
  - validace
    - security koncept
    - využití stávajících mechanismů
    - dodržení secutity standardů
  - architektonický návrh
    - funkční a technologický návrh
  - definice testů
- **SD (Solution Design)**
  - rozpracování vstupů z PD
- **I (Implementace)**
  - dodržování security guidelines
  - code review (dle OWASP)
  - penetrační testy

Riziko vs. náklad

- **Obecný princip**
  - vzhledem k nastaveným procesům jsem schopen definovat úroveň bezpečnosti vhodnou pro konkrétní aplikaci
- **Pohled oddělení security**
  - maximálně zabezpečená aplikace
  - důraz na co nejmenší počet incidentů
  - kompletní dohled nad systémem (auditování, logy)
- **Pohled businessu**
  - důraz na nízké implementační náklady
  - požadavek na uživatelskou přívětivost
- **Praxe**
  - vyvážený přístup ke stupni zabezpečení aplikace
    - náklady vs. riziko
    - uživatelská přívětivost vs. riziko

Eliminace rizik

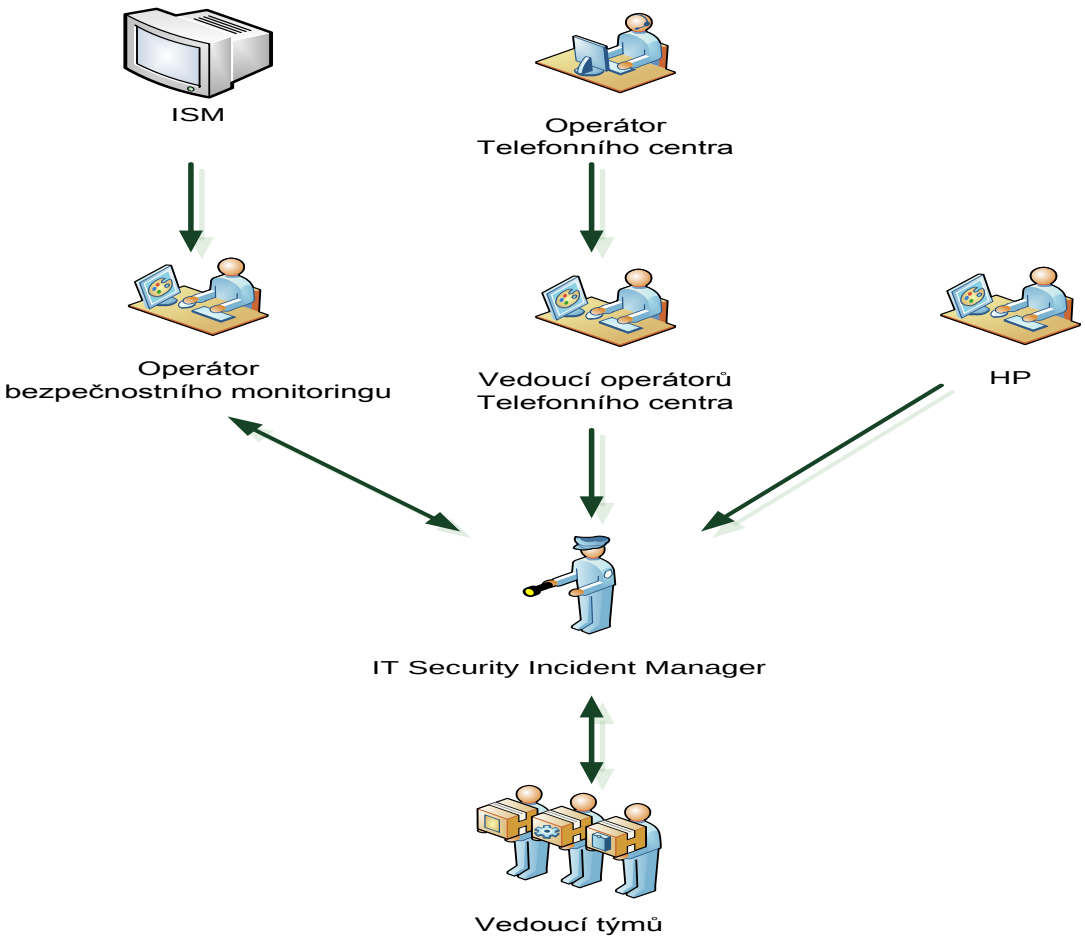
- **Technologické**
  - PKI
  - FDS
  - SSL
  - security coding standards

- **Procesní**
  - dvoukanálová autorizace (internet, mobilní operátor)
  - kontrola auditních logů (ISM)
  - změna business procesů (místo přes internet návštěva pobočky)

- **Aktivní zapojení uživatele do procesů bezpečnosti**
  - kontrola IP adresy a času posledního přihlášení
  - detaily transakce v jednorázovém hesle
  - message box
  - customizace přihlašovací stránky
  - desatero bezpečnosti uživatele internetu

- **Od 1.1. 2010 výrazně odlišný přístup k řešení případných reklamací**
  - zhoršená pozice banky
  - důkazní břemeno je na bance

Bezpečnost v produkčním prostředí



Další kroky, plán

- **Fraud Detection System**
  - implementace komplexního řešení
  - databáze známých útoků
  - white list, black list
- **Alokace budgetu**
  - definice speciálního budgetu na pokrytí případných incidentů
- **Další zkvalitnění vyvíjeného kódu v aplikacích z hlediska bezpečnosti**
  - důraz na znalosti a zkušenosti vývojových pracovníků v oblasti bezpečnosti
  - další rozvoj znalostí a zkušeností pracovníků
- **Procesní zlepšení**
  - optimalizace procesů a to jak ze strany business tak IT
  - návrh procesu a jeho důsledná kontrola

Děkuji za pozornost