AEC
DATA SECURITY

Bezpečnost ve vývoji webových aplikací

Security 2010

Daniel Kefer
17. 02. 2010

Představení

- Daniel Kefer:
  - IT Security Consultant
  - zaměstnanec AEC, spol. s.r.o. (od r. 2005)
  - realizace penetračních testů a bezpečnostních auditů
  - garant kompetence bezpečného aplikačního vývoje

Agenda

- Aktuální stav bezpečnosti webových aplikací
- Bezpečnost ve vývoji/životním cyklu webových aplikací
- Case study

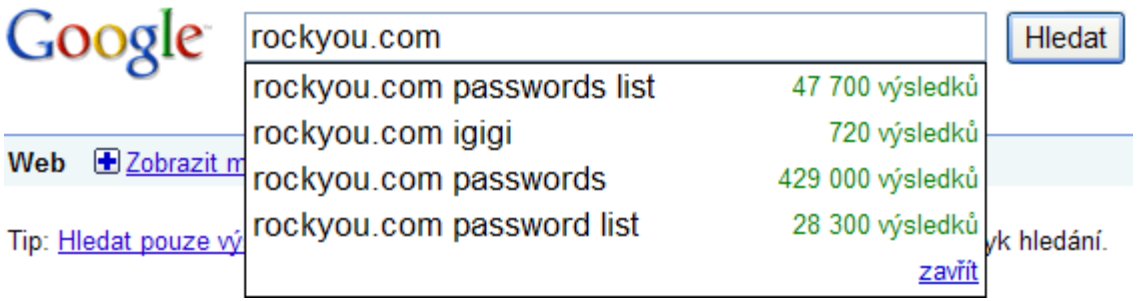
Aktuální stav bezpečnosti aplikací

- Pozorování konzultačních společností:
  - Gartner: 80 % úspěšných útoků je realizováno skrz webové aplikace
  - Forrester: 36 % zákazníků nevyužívá služby poskytované webovými aplikacemi z důvodu o svoji bezpečnost
  - McAffee: Průměrná cena narušení bezpečnosti střední firmy v roce 2008 byla 43 000 dolarů
  - Verizon: 25 % útoků je detekováno až v řádech týdnů, 49 % dokonce v řádu měsíců

=> Provozování webových aplikací je spojeno s riziky zásadního charakteru

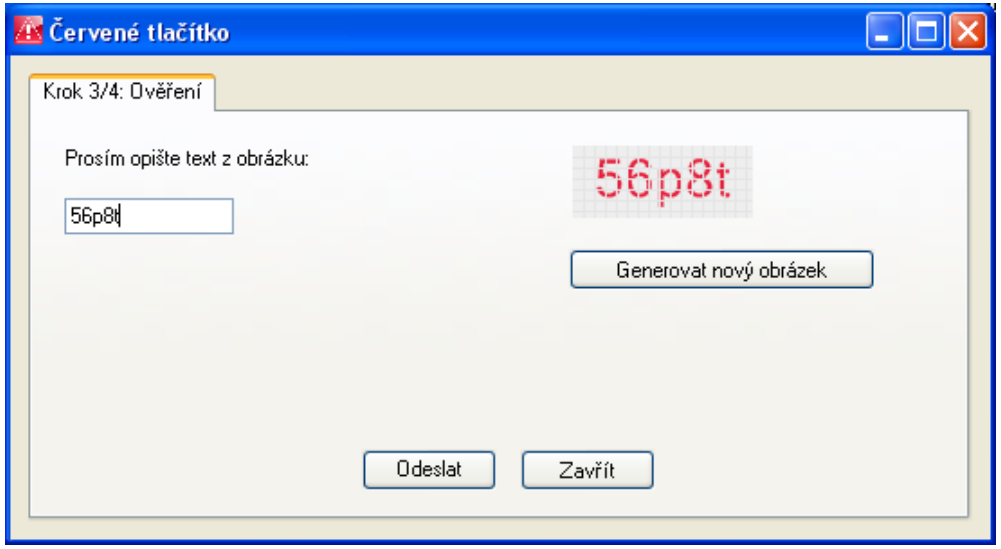
Aktuální stav bezpečnosti aplikací – příklad

- prosinec 2009: SQL Injection – únik uživatelských účtů:
  - pravděpodobně slovenský hacker „Igigi“
  - nejznámější hack: rockyou.com - přes 32 milionů účtů
  - hacknuto mnoho CZ a SK webů během 2 týdnů
  - csfd.cz, shoptet.cz, rozzlobenimuzi.com, zoner.cz, union.sk, denik.cz, atlas.sk, aaaauto.cz, games.tiscali.cz, auto.cz, azet.sk...
  - hesla uživatelů ukládána v plain textu nebo pomocí slabých algoritmů



Červené tlačítko

- Legislativa?
- Phishing?
- Bezpečnostní opatření?



GET http://ohlaste.horkalinka.cz/redButton/insert.asp?text=pokus&url=&date=11.2.2010+1%3a08%3a09 HTTP/1.1
Host: ohlaste.horkalinka.cz
Proxy-Connection: Keep-Alive

Aktuální stav - naše pozorování

- Zranitelnosti z pen. testů:
  - CRITICAL: 42 % projektů
  - HIGH: 88 % projektů
- Bezpečnost při vývoji:
  1. Neřešena
  2. Pouze penetrační testy
  3. Řešena od začátku vývoje, ale nedůsledně
- Oddělení bezpečnosti (pokud je vybudováno) je nedostatečně zapojeno do oblasti vývoje aplikací

Proč bezpečnost != penetrační testy

- Penetrační testy:
  - zhodnocení bezpečnosti z omezeného pohledu
  - důraz hlavně na nefunkcionální vlastnosti aplikace
  - ve vývojovém cyklu až v testovací fázi
  - odražejí stav aplikace pouze v konkrétním čase za specifických podmínek

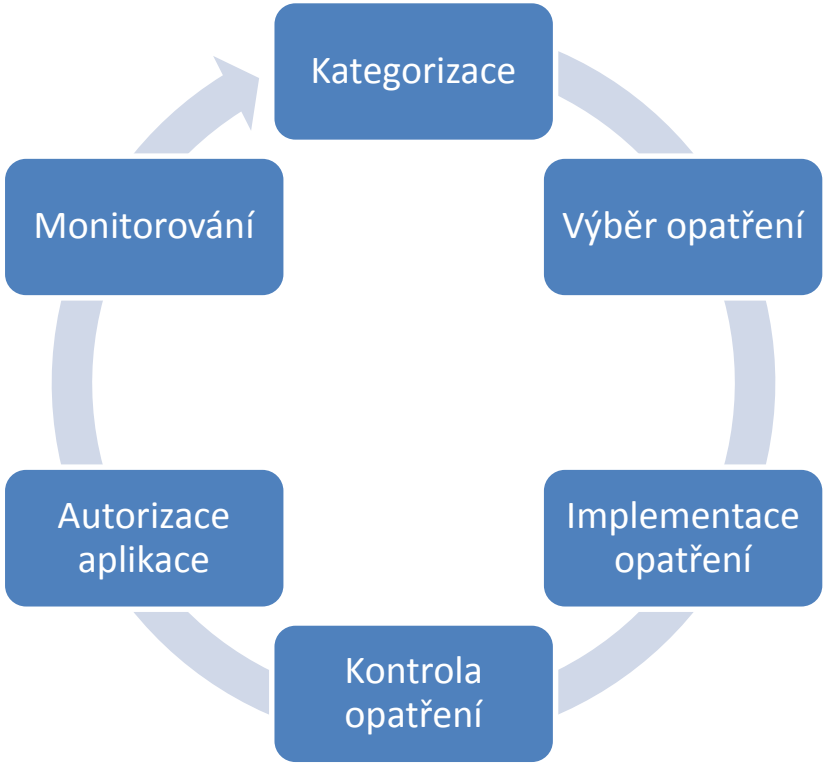
- Nákladná oprava nalezených zranitelností
  - chyby v designu
  - pracnosti vývojářů
  - zadavatel X dodavatel

Bezpečnost v SDLC

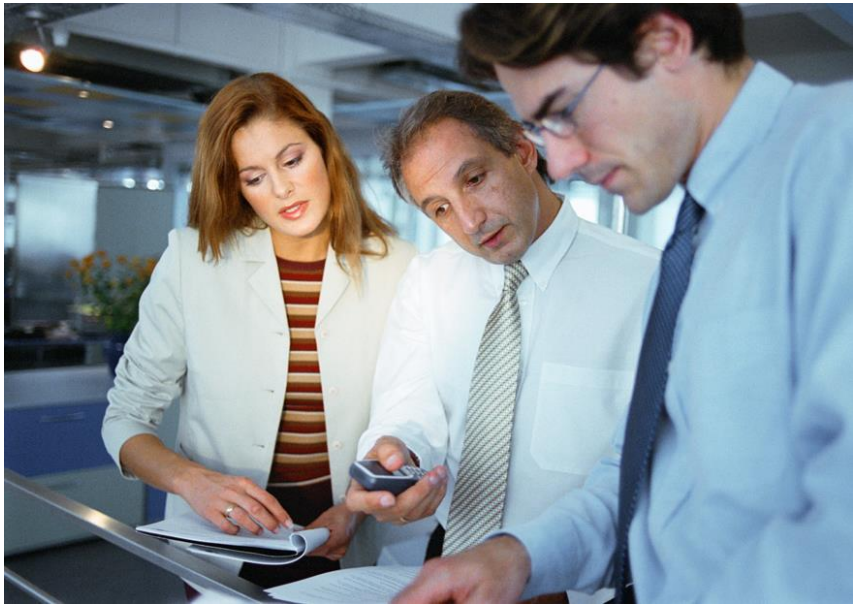
- Zapojení bezpečnosti do vývoje aplikací:
  - již od analytické fáze
  - na míru specifikům a metodikám organizace
  - postaveno na základě obecně uznávaných metodik:
    - NIST
    - OWASP
    - ISO/OSI
- Vhodné pro:
  - Aplikace vyvíjené in-house
  - Dodávané aplikace
  - Krabicová řešení

Bezpečnost v SDLC

- Bezpečnostní oblasti řešení:
  - Technické – Kontrola přístupu, Ochrana aplikace a komunikace...
  - Provozní – Bezpečnost obsluhy, Incident Response...
  - Plánovací – Analýza rizik, Autorizace aplikace...
- Princip zapojení bezpečnosti:



Bezpečnost v SDLC - Rizika



- Neefektivita procesu
- Vznik „bílých míst“

Omezení rizik:

- Důležité je nepodcenění analytické fáze
- Důsledné naplánování procesů a nastavení očekávání
- Je vhodné stavět na zavedených normách, standardech a metodikách
- Využití zkušeností z již realizovaných projektů

Case Study – Vodafone Park

Case Study – Vodafone Park

- AEC dodavatelem bezpečnosti již od analytické fáze projektu
- Nejdůležitější aktivity:
  - Analýza business požadavků
  - Školení a konzultace vývojářům
  - Aktivní identifikace rizik po celou dobu projektu
  - Penetrační testy
- Přínosy:
  - Důvěryhodnost portálu - posílení dobrého jména společnosti
  - Výrazné ponížení rizik finančních ztrát spojených s provozem portálu

Závěr

- Aktuální situace může mít pro firmy i důsledky likvidačního charakteru
- Je potřeba více pochopení mezi businessem a bezpečností
- Realizované případy ukazují, že zapojení bezpečnosti do vývoje aplikací přináší:
  - nižší TCO
  - kratší ROI
  - snížení provozních rizik
  - posilování dobrého jména společnosti
  - ...

AEC
DATA SECURITY

Dotazy?

Děkuji za pozornost!