Obhajoba bakalářské práce

Security of small business e-commerce sites

Karel Kohout (xkohk02@vse.cz)

Vedoucí: Ing. Jaromír Veber
Oponent: Ing. Martin Dvořák

Motivace a cíl práce

Motivace:

- klesající náklady na napadení, rostoucí počet internetových obchodů,
- internetový obchod jako systém „na pomezí“ (veřejná stránka, informační systém),
- data jako cenná komodita a závazek,
- pracovní zkušenosti.

Cíl práce:

- stanovit nejběžnější problémy se zabezpečením malých internetových obchodů se zaměření na EU,
- ověřit, zda se zmíněné problémy vyskytují v reálně používaných aplikacích,
- prozkoumat, jak by zabezpečení mohlo ovlivnit zákazníky.

Základní body a literatura

1. Úvod do problematiky bezpečnosti internetových obchodů a obchodování na internetu, omezení práce
   - BISKUP, J. Security in computing systems
2. Teoretické právní a technické předpoklady bezpečného obchodu
   - Komunitární právo EU (směrnice a nařízení)
   - ČSN/ISO/IEC 2700x, NIST (800, FIPS)
   - STUTTARD, D. – PINTO, M. The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws
   - SNYDER, C. – SOUTHWELL, M. Pro PHP Security
3. Aplikace předpokladů na zhodnocení bezpečnosti sedmi aplikací
   - DAVIS, C. – SCHILLER, M. – WHEELER, K. IT Auditing: Using Controls to Protect Information Assets
4. Možný vliv zabezpečení na zákazníky obchodu
   - SUH, B. – HAN, I. The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce [online]

Zhodnocení bezpečnosti

- Původní předpoklady (honeypot).
- Výběr software, stanovení kritérií (str. 38):
  - **ošetření vstupu** (účinnost, CSRF, spam – ochrana, MIME),
  - **uživatelské účty** (oddělení rolí, únik dat, už. práva, nev. e-maily),
  - **obecné zabezpečení** (updaty, známé chyby, mailing list, pluginy)
  - **dokumentace a právní problémy** (informace, doporučení, bezpečná instalace, souhlas uživatelů)
  - **„správné postupy“** (PHP, výjimky, komentáře, logy)
  - **ochrana osobních údajů** (šifrování, session, kryptografická bezpečnost).
- Metody ověřování:
  - kontrola vybraných zdrojových kódů, souborů na disku a databáze,
  - prověření logů webového serveru,
  - analýza HTTP paketů a jejich úpravy,
  - kontrola stránek a dokumentace aplikací.

Vliv zabezpečení

- Krátký dotazník, výběr ze 4 odpovědí.
- 12 otázek, cíl:
  - podpořit některá tvrzení (uchovávaná data),
  - zjistit, jak uživatelé vnímají zabezpečení (viditelné, skryté).
- Okruhy:
  - ochrana osobních údajů (co, komu, za jakých podmínek),
  - rozpoznání (ne)bezpečné stránky,
  - vliv „důvěry“,
  - účinnost sledování.

Výsledky a vlastní přínos

Zabezpečení internetových obchodů (str. 45, str. 55):

- žádný obchod není bezpečný,
- obrovské rozdíly mezi obchody bez ohledu na množství uživatelů,
- některé aplikace jsou naprosto nevhodné.

Výsledky hodnocení (maximum 24):

Magento	OpenCart	Oxid	Prestashop	Ubercart	VirtueMart	Zen Cart
15	9	17	9	21	14	12

Vnímání zabezpečení:

- nízká schopnost poznat bezpečnou stránku,
- „prodej“ zabezpečení,
- nutné alternativy ke cookies.

Omezení práce, možnosti rozšíření

Omezení:

- sledovaný software,
- rozsah studie.

Rozšíření:

- cílená studie (jak ovlivnit důvěryhodnost internetového obchodu),
- reálné procento napadených aplikací.

Dodržování standardů W3C a bezpečnost

Otázka

Nepřináší fakt, že se doposud Microsoft nechtěl podřídit standardům v oblasti webových stránek (HTML a XML) a obchodníci tak museli nechat upravovat své webové stránky zvlášť pro Explorer a ostatní prohlížeče další určitá bezpečnostní rizika?

- Dodržování standardů, úpravy (podmíněné komentáře), preference při vývoji.
- Aktuální rizika
  - přímá: ohrožení uživatele (web fungující jen s MSIE 6), větší rozsah kódu, nestandardní postupy (zobrazení PNG).
  - nepřímá (důsledky): Adobe Flash, MS Silverlight.

Rizika outsourcingu

Otázka

Autor předpokládá, že některé prvky menšího podniku (servery a jejich administrace) jsou outsourcovány. Jaká rizika outsourcing přináší?

- ISO 27001: A.10.2 [2, str. 152]
- Rizika (obecná, neřešitelná): informační asymetrie (problém principal, agent), asymetrie ve vyjednávací síle, schopnost dokonale zpracovat kontrakt, náklady na soudní spor.
- Rizika (řešitelná): závislost na dodavateli, ztráta schopností a dovedností, inovace.
- SLA, výše odpovědnosti dodavatele, vymahatelnost.

CAPTCHA

Otázka

Lze CAPTCHA systémy dnes stále ještě považovat za efektivní nástroj vzhledem k pokroku v oblasti OCR o které jsou nejnovější exploity vybaveny?

-  [1]
- CAPTCHA = Completely Automated Public Turing Test to Tell Computers and Humans Apart [1]
- Hrozby: OCR, rozpoznání hlasu, chybné implementace, levná pracovní síla.
- Efektivní CAPTCHA:
  - Požadavky: snadno řešitelné člověkem, obtížně počítačem; pevná minimální doba řešení.
  - Omezení: nestandardní situace, náročnost na „kulturní“ povědomí, inteligenci, ...
  - Řešení: „sbírání bodů“ (viz spamový filtr).

[1] Zdroj: `gmail.com`.

Doporučené aplikace

Otázka

Která z Vámi analyzovaných aplikací pro e-obchod je v EU nejvíce používaná, a jak je to s její bezpečností.

- Problematika určení nejpoužívanější aplikace (obrat, rozpoznání).
- Výběr software (str. 43):

Název	Popularita (dle vyhledávačů, v tisících)
Magento	7250
OpenCart	563
Oxid eshop community edition	3720
Prestashop	2250
Ubercart (Drupal)	7460
VirtueMart (Joomla)	18900
Zen Cart	17800

- Dle instalací: Zen Cart, VirtueMart. Dle obratu: Oxid eshop, Magento (komerční).

Doporučené aplikace

Otázka

Kterou z vámi analyzovaných aplikací byste naopak doporučil právě z hlediska bezpečnosti.

- Oxid e-shop, Ubercart.

Eliminace konkurence

Otázka

Kterým útokem byste útočil na konkurenční e-shop za účelem eliminace konkurence?

Problémy:

- konkurence (více e-shopů),
- účelnost útoku (poškození trhu),
- riziko,
- náklady.

Útoky (říjen - prosinec):

- zvýšení nákladů,
- snížení obratu.

Zdroje I


AHN, Luis von, BLUM, Manuel, LANGFORD, John: Telling Humans and Computers Apart (Automatically) Or How Lazy and Lazy Cryptographers Do Ai, Communications of the ACM (rok 2007, svazek 47, strana 60). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.67.4530&rep=rep1&type=pdf [dostupné 18.8.2010].


DOUCEK, Petr, NOVÁK, Luděk, SVATÁ, Vlasta, Nedomová, Lea: Řízení bezpečnosti informací. Professional Publishing, Praha, 2008. ISBN 978-80-86946-88-7.