Silent Signal Kft.

WebShop Tuning

Szabó Péter

Varga-Perke Bálint

2009.11.21.

Témáink

- Bevezető
- Kik vagyunk
- Az IT biztonság üzleti kockázatai
- Vizsgálati megközelítések webáruházaknál
- Általános sebezhetőségek
- Open-source vs. fizetős vs. In-house fejlesztés
- SSL titkosítás (Tényleg feltörték?)

SILENT SIGNAL

Bevezető

- „Normál” áruháznál egyértelmű a biztonság
- Webáruháznál miért nem?
- Reménykedni: Lehet!
- Időt visszaforgatni: NEM lehet!

Pár felvetés, amire az előadáson válaszolni fogunk:

- Milyen valódi biztonsági kockázatok fenyegetik az online elérhető webáruházakat?
- Milyen közvetlen és közvetett károkat okozhat a nem megfelelő védelem?
- Miért fontos a hitelesség és a titkosság a kereskedők és a vásárlók számára?

Az informatikai kockázat = Üzleti kockázat!

Kik vagyunk

Információtechnológia

↓

Informatikai biztonság

↓

Etikus hackelés

IT biztonsági tanácsadás

IT biztonsági oktatás

Csapatunk

- Etikus hackelési szaktudás
- IT biztonsági szabványok, előírások ismerete
- Hálózati szakértelem
- IT projekt-menedzsment szaktudás

Értékeink

- Több éves tapasztalat az IT Security szakterületen
- Hacktivity 2004-2005 wargame győztes
- Goldenblog 2009. IT kategóriagyőztes
- Hacktivity 2009. Hack the Vendor győztes
- Rendszeres előadások, cikkek (Pl. IIR, Hacktivity, IT business, EESTEC, New Tech. Meetup)

Etikus hackelés

- Legális autófeltörés
- Teljes mértékben a megbízó adja a szabályokat
- Többfajta megközelítés, szerepkör
  - Hatókör
  - Információ bázis
  - Agresszivitás
  - Kiindulási pont
- Nem kihasználjuk, hanem feltárjuk a biztonsági réseket

Tegye próbára IT rendszerét, és előzze meg a biztonsági incidenseket!

IT biztonság üzleti kockázatai

- Jogi háttér
  - Az elektronikus kereskedelmi szolgáltatások (2001. évi CVIII. törvény)
  - A távollevők között kötött szerződésekről szóló 17/1999. (II. 5.) Korm. rendelet
  - A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény
- **Az ügyfélbizalom megszerzése és megtartása**
- **Adatkiszivárgás, adatvesztés (közvetett anyagi kár)**
- **Szolgáltatás fennakadás (közvetlen anyagi kár)**
- **Szabadvásár (közvetlen anyagi kár)**

Tényleg kakukktojás a mi előadásunk?

Vizsgálati megközelítések

- **Black-box vizsgálat**
  - Információ nélkül, egy külső támadó lehetőségei a webáruház infrastruktúráján
- **Grey-box vizsgálat**
  - Egy regisztrált felhasználó támadási lehetőségei a webáruház infrastruktúráján
  - Egy volt rendszergazda, fejlesztő támadási lehetőségei a webáruház infrastruktúráján
- **White-box vizsgálat**
  - Üzemeltetői, fejlesztői oldalról történő vizsgálat, a teljes rendszer ismeretében

SILENT SIGNAL

A technika ördögei

- **Webshop = Komplex IT rendszer**
  - Hibamentes rendszer létrehozása szinte lehetetlen
- **Minden felhasználó potenciális támadó lehet**
  - Nem tudjuk megkülönböztetni Manyi nénit egy zombihadseregtől
- **Minden felhasználói kezelőelem fegyverré válhat egy támadó kezében**
- **Egy webalkalmazás jó bejutási pont lehet a háttérinfrastruktúrához**
  - Belső adatbázisok, fájlszerverek, munkaállomások

A támadások céljai

- **Zombihadsereg toborzása**
  - A megtámadott webkiszolgálókból
  - A megtámadott kiszolgálók látogatóiból
- **Adatlopás, adathalászat**
  - Személyes adatok
  - Pénzügyi információk
- **Deface**
  - Politikai, társadalmi aktivizmus
  - Hitelrontás
  - Szórakozás, önkifejezés...

A támadások lélektana

- **Automatizált, nagy kiterjedésű támadási hullámok**
  - Akár több millió érintett webhely
  - A „Miért támadnának meg pont engem?” kérdés ma már értelmetlen
- **Sok támadás már kompromittált gépről zajlik**
  - A valódi elkövetők lenyomozhatatlanok
- **A támadások legtöbbször észrevétlenek maradnak**

A biztonság ára

- **Nem Ön az egyetlen, aki webáruházat nyit**
  - A munka oroszlánrészét valaki már elvégezte
  - Miért fizetnénk a kerék újrafeltalálásáért?
- **Minden egyedi fejlesztéshez szükséges:**
  - Tudás
  - Idő
  - Pénz
- **A drágább nem mindig jobb!**

SILENT SIGNAL

A biztonság ára

- **A webfejlesztő piac hemzseg a kóklerektől**
  - Sufnituning fejlesztések, enterprise köntösben
- **„Hány biztonsági hibajavítást végeztek az előző verzió óta?”**
- **Használjunk ellenőrzött eszközöket**
- **Nem egyszeri költség!**
  - Frissítések és felügyelet nélkül védtelenek vagyunk!

SILENT SIGNAL

A titkosításról

- **Felhasználói adatok, elsősorban jelszavak**
  - Az ügyfél jelszavához az üzemeltetőnek semmi köze!
  - Titkosítás nélkül a komplex jelszavak sem érnek semmit
  - Az egyedi fejlesztésű eljárások soha sem megbízhatóak
- **Hálózati forgalom**
  - SSL

SILENT SIGNAL

SSL

- **Hitelesítés**
  - **Tudom, kivel beszélek**
- **Titkosítás**
- **Biztonságos?**
  - **Ha jól csinálják, igen!**
  - **Az újságíróknak nem kell mindent elhinni...**

SILENT SIGNAL

SSL – Mire ügyeljünk?

- **Megbízható, jól ismert tanúsító szervezet választása**
- **Ne csak a bejelentkezéskor használjuk!**
  - **Munkamenet azonosítók**
  - **Privátszféra-védelem**
- **Nem csodaszer**
  - **Egy rosszul megírt szoftveren az SSL sem segít!**

SILENT SIGNAL

Összefoglalás

- A biztonság NEM felesleges költség
- Alacsony biztonsági szint = magas üzleti kockázat
- Bárki támadási célponttá válhat
- Használjuk ellenőrzött rendszereket
- Nem egyszer kell jó rendszert alkotni, hanem folyamatosan – FRISSÍTÉSEK
- Titkosítás kiemelten fontos

Ingyenes vizsgálat

INGYENES VIZSGÁLATI LEHETŐSÉG!*

CSAK MOST A WEBSHOP TUNING KONFERENCIÁN!

* Feltételek, amit nem lehet elolvasni.

Ingyenes vizsgálat

Feltételek:

- **1 cég csak 1 webáruház vizsgálatát kérheti**
- **A vizsgálat egy alap black-box vizsgálat, mely a jellemző súlyos hibákra koncentrál**
- **A vizsgálat végeredménye egy prezentáció, ahol a tapasztalatok bemutatásra kerülnek**
- **A vizsgálatokat az ügyféllel egyeztetett időpontban 2010. I. negyedévében végezzük el**
- **Csak az első 10 jelentkezőnek tudjuk biztosítani ezt az ingyenes vizsgálati lehetőséget**

Jelentkezés: info@silentsignal.hu

Köszönjük megtisztelő figyelmüket!

SILENT SIGNAL

VÉSZJELZÉS HELYETT...

Szabó Péter

szabo.peter@silentsignal.hu

Varga-Perke Bálint

vpbalint@silentsignal.hu

www.silentsignal.hu

info@silentsignal.hu