Obsługa incydentów bezpieczeństwa: część I, z punktu widzenia menadżera.

Przemysław Skowron
OWASP Poland Leader

Alior Bank S.A.
przemyslaw.skowron@gmail.com

OWASP
2010.03.17

The OWASP Foundation
http://www.owasp.org

Agenda

- OWASP News w Warszawie

- Co to jest incydent bezpieczeństwa?
- Jakie są przyczyny incydentów?
- Jak przygotować się do obsługi incydentu?

- Podsumowanie

OWASP News w Warszawie

- Współpraca z ISSA Polska

- Ilu mamy członków Fundacji OWASP na sali?
- Nowa jakość materiałów:
  - prezentacje, audio-video (trwa montaż)
- OWASP AppSec Research 2010 – Szwecja; ktoś chętny?

Co to jest incydent bezpieczeństwa?

Incydent związany z bezpieczeństwem informacji jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

(tłumaczenie wg PN-ISO/IEC 27001:2007)

Co to jest incydent bezpieczeństwa?

- Aplikacje webowe

To **nie tylko** SQL Injection, XSS czy CSRF

Co to jest incydent bezpieczeństwa? - II

- Aplikacje webowe
  - Uwierzytelnienie (brute force blokujący konta)
  - Zarządzanie sesją (identyfikator sesji w URLu)
  - Kontrola dostępu (+1 do id)
  - Walidacja danych wejściowych / kodowanie wyjściowych (phishing, zmiana hasła użytkownika)
  - Kryptografia (tęczowe tablice)
  - Obsługa błędów (domyślne zabranianie)
  - Ochrona danych (nagłówki cache)

Co to jest incydent bezpieczeństwa? - III

- Aplikacje webowe
  - Bezpieczna komunikacja (zwykły http do zew. komponentów)
  - Bezpieczeństwo protokołu HTTP (atrybuty ciastek)
  - Bezpieczna konfiguracja (pliki konfiguracyjne dla wszystkich)
  - Złośliwy kod (☺)
  - Bezpieczeństwo wewnętrzne (zmiana uprawnień użytkownikowi)

  - Logika biznesowa (!)

Jakie są przyczyny incydentów?

- *„Incident response happens when your secure development lifecycle fails.”* – Dave Aitel, Keynote na FIRST 2010

- **OWASP Application Security Verification Standard**
  - Wkrótce pojawi się tłumaczenie na j. polski

Jakie są przyczyny incydentów? - II

- Nie testujemy webapp/środowiska bo:
  - mamy IPS za „*milion*"
  - korzystamy z bezpiecznej technologii
  - domyślna konfiguracja jest bezpieczna
  - integrator skonfigurował produkty zgodnie z dobrymi praktykami
- Bolączki testów:
  - często testy typu *blackbox* – czego się boimy?
  - testy przeprowadzane za pomocą skanerów
- Błąd ludzki

Jak przygotować się do obsługi incydentu?

Incydenty bezpieczeństwa zdarzają się kiedy jesteśmy nieprzygotowani do ich obsługi ☺

Jak przygotować się do obsługi incydentu?

- Utworzyć CSIRT:
  - Kompetencje
  - Szkolenia
  - Narzędzia
  - **Plan obsługi incydentu!** ☺
- Stworzyć monitoring:
  - Aktywny, pasywny
  - Trendy
- Utrzymywać stan gotowości

Bonus: Zapytanie HTTP

http://www.issa.org.pl/content/view/154/1/

GET /content/view/154/1/ HTTP/1.1
Host: www.issa.org.pl
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; pl; rv:1.9.2) Gecko/20100115 Firefox/3.6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: pl,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-2,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.issa.org.pl/
Cookie: 7a240057dfdd3a69dc9af637d5732a23=13ff3e5c83561ad767fdb4d4a317d1ce; mosvisitor=1; __utma=50012606.1231250683.1268738717.1268738717.1268738717.1; __utmc=50012606; __utmz=50012606.1268738717.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Cache-Control: max-age=0

Bonus: Zapytanie HTTP w logach

http://www.issa.org.pl/content/view/154/1/

```
GET /content/view/154/1/ HTTP/1.1
Host: www.issa.org.pl
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; pl; rv:1.9.2) Gecko/20100115
    Firefox/3.6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: pl,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-2,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.issa.org.pl/
Cookie: 7a240057dfdd3a69dc9af637d5732a23=13ff3e5c83561ad767fdb4d4a317d1ce;
    mosvisitor=1; __utma=50012606.1231250683.1268738717.1268738717.1268738717.1;
    __utmc=50012606;
    __utmz=50012606.1268738717.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Cache-Control: max-age=0
```

Bonus: Zapytanie HTTP - II

https://test.pl/test.asp

POST https://test.pl/test.asp HTTP/1.1
Host: test.pl
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; pl; rv:1.9.2) Gecko/20100115 Firefox/3.6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: pl,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-2,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: https://test.pl/index.asp
Content-Length: 7
Cookie: SSID=A84fvuzYVb6gN9xTX

count=6

Bonus: Zapytanie HTTP w logach - II

https://test.pl/test.asp

POST https://test.pl/test.asp HTTP/1.1
Host: test.pl
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; pl; rv:1.9.2) Gecko/20100115 Firefox/3.6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: pl,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-2,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: https://test.pl/index.asp
Content-Length: 7
Cookie: SSID=A84fvuzYVb6gN9xTX

count=6

Obsługa incydentów bezpieczeństwa: **część II,**
z punktu widzenia eksperta już wkrótce na
SEConference 2010.

Podsumowanie

- Podziękowania:
  - Zaproszenie: ISSA Polska (Hubert Pilarski!)
  - Hosting: Ernst&Young
  - **Uczestnicy !**

- Następne spotkanie (prawdopodobnie) w maju! – Kraków, a może i Warszawa? ☺

- Zapraszam na maillistę **owasp-poland**!

Dziękuję za uwagę: do zobaczenia! ☺

http://www.owasp.org/index.php/Poland