Tavola Rotonda: "Sicurezza Informatica Open Source, Codice Proprietario e Interoperabilita'"

Moderatore:
Marco Morana, OWASP

Relatori:
Feliciano Intini, Microsoft Italia
Gianstefano Monni, Ablativ Scrl
Fabio Panada, IBM ISS
Domenico Presenza. Engineering
Paola Tamburini, IBM ISS

OWASP

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

Agenda

- Introduzione dei relatori
  - Presentazione dei relatori (breve biografia)
- Discussione dei temi su sicurezza open source vs. codice proprietario e interoperabilita'
  1. Sicurezza del software Open Source Software (OSS)
  2. Sicurezza informatica e diversita' del software
  3. Rischi dovuti all integrazione/interoperabilita'
  4. Conseguenze dovute gestione delle patches
  5. Costi di gestione della sicurezza
- Conclusione
  - Indagine

Domanda #1 Per I Relatori

- **Tema: L'accesso al codice sorgente come criterio per decidere se open source e' piu sicuro del codice proprietario**
  - La direttiva del parlamento europeo A5-0264/2001 considera il software aperto piu visibile e quindi piu sicuro del software chiuso (proprierario)
  - Secondo Whitfield Diffie co-inventore della crittografia pubblica l'assunzione che il software commerciale e' piu' sicuro perche segreto non ha senso
- **Domanda**
  - E' l'accesso al codice sorgente garanzia sufficiente per cosiderare il software open source piu sicuro del software proprietario?

Domanda #2 Per I Relatori

- **Tema: L'adozione di software e sistemi eterogenei (open source e non) riduce i rischi**
  - Nel 2004 la Comunita Europea, esaminando il tipo di software acquisito dai vari governi, rivelo' una predominananza di sistemi basati su architecture Intel praticamente favorendo una piattaforma dominante. Nel 2002 il Governo Tedesco si e mosso vs. sistemi Linux e OpenLDAP. Nel 2007 il Governo Francese ha speso circa 11% del budget per ICT per sistemi open source.
- **Domanda:**
  - Quale e' stato l' impatto dell' adozione di sistemi eterogenei, cioe' sia open source e software proprietario sullo stato della sicurezza informatica dei vs. clienti o azienda?

Domanda #3 Per I Relatori

- **Tema: La domanda per OSS e' in crescita ma non lo sono le verifiche che il software OSS e' sicuro**
  - Una indagine tra 328 managers USA in IT nel 2008 trova che il 50% usano applicazioni open-source. Gartner prevede una crescita di OSS del 88% per il 2011
  - Secondo un indagine di Fortify Software, la maggioranza del OSS non e' testato per la presenza di vulnerabilita' prima di essere messo in produzione
- **Domanda:**
  - Ritenete necessaria l'adozione di test di sicurezza per verificare la sicurezza del software open source prima dell' integrazione e messa in produzione?

Domanda #4 Per I Relatori

- **Tema: I tempi di sviluppo delle patches e l' impatto sulla sicurezza OSS vs. codice proprietario**
  - Nel Giugno 2004 il US CERT raccomanda l'uso di Mozilla browser invece di IE perche' Microsoft ha aspettato 9 mesi prima di pubblicare una patch per IE
  - C'e voluto un anno e 9 mesi per Debian per scoprire una vulnerabilita' in OpenSSL per un bug introdotto durante un debugging di libreria
- **Domanda**
  - I tempi per la gestione delle vulnerabita' del software, open source o commericiale sono un fattore di rischio? (e.g. impatti dovuti ai tempi di sviluppo delle patches, test e installazione)

Domanda #5 Per I Relatori

- **Tema: Costi per la gestione della vulnerabilita' OSS e proprietario**
  - L' uso di OSS comporta spese per la gestione e supporto come per sistemi proprietari. I costi di sviluppo delle patches, in genere ricadono su chi produce software: il costo medio per lo sviluppo di una patch non OSS costa 100,000$ (Microsoft) e rimediarla durante la fase di progetto costa 100 volte di meno che rimediarla con una patch in produzione (IBM). I costi di gestione ricadono sull'utente: per esempio patching 1000 servers puo costare fino a 300,000 $ (Gartner).
- **Domanda**
  - Chi si deve assumere i costi della gestione delle vulnerabilta' del software? Ridurre i costi di gestione delle vulnerabilita' e' un argomento valido per rimediare le vulnerabilta' durante lo sviluppo del software?

OWASP

Conclusione: Indagine Fra I Relatori

- Quanti di voi si occupa di aspetti di vulnerabilita delle web applications per la vs. azienda o clienti?
- La vs. azienda/cliente utilizza librerie software open source per la sicurezza o sistemi operativi/servers basati su technologia open source?
- Quanti fra le vostre aziende/clienti hanno adottato pratiche per validare e sviluppare software sicuro come, standards per programmazione sicura, analisi del codice e penetration test?