

Cosa si può chiedere e cosa si può pretendere da un fornitore di servizi di sicurezza informatica

Autore: **Raoul Chiesa (OPST, OPSA)**

**Socio Fondatore, Membro del Comitato Direttivo CLUSIT
Board of Directors Member: ISECOM, OWASP Italian Chapter**

ROMA, 11 GIUGNO 2008



Indice

- ◆ Premessa
- ◆ Una storia di vita vissuta
- ◆ Errori tipici
- ◆ Altre valutazioni da fare
- ◆ Conclusioni
- ◆ Riferimenti
- ◆ Q&A

Il relatore – Raoul Chiesa

- ◆ **Director of Communications** at ISECOM (Institute for Security and Open Methodologies, USA)
- ◆ **OSSTMM Key Contributor, Project Manager di HPP**
 - Open Source Security Testing Methodology Manual
 - Rilasciato nel gennaio 2001
 - Più di 3 milioni di downloads
- ◆ **Docente di IT Security** presso varie Università e Master di InfoSec.
- ◆ **Speaker** ad eventi di sicurezza nazionali ed internazionali.
- ◆ **Membro del Comitato Direttivo: CLUSIT, ISECOM, Telecom Security Task Force (TSTF.net), OWASP Italian Chapter.**
- ◆ **Consulente** per le Nazioni Unite sul cybercrime presso l'**UNICRI (United Nations Interregional Crime & Justice Research Institute).**



Premessa

I'm not a lawyer... (disclaimer)

- **Non sono** una figura di stampo legale.
- Di conseguenza, questo intervento vuole più che altro **fornire esperienze di vita vissuta**.
- Diverse volte, infatti, mi è capitato di **supportare** aziende clienti nella **corretta selezione** del “Fornitore di IT Security”.
- Non dimentichiamoci inoltre l'**enorme e variegato mondo** (e mercato) rappresentato dal termine “IT Security”: nei prossimi venti minuti mi focalizzerò su quelle tematiche proprie della mia nicchia di settore (Penetration Testing, Computer Forensics, Risk Analysis).
- Ciò nonostante, da queste **esperienze** sono scaturite delle **lezioni**, che ho cercato di sposare in **principi** da seguire.

Storie di vita vissuta

Storie di vita vissuta - 1

- Penetration Testing.
 - ◆ All'interno di un progetto più ampio, mi fu richiesto di agire come "Selezionatore di Tiger Team" per un'azienda di grandi dimensioni.
 - ◆ La volontà del Cliente era di selezionare **2 team** appartenenti a Fornitori differenti, i quali avrebbero operato **senza essere a conoscenza** l'uno dell'altro.
 - ◆ Il contratto prevedeva 4 Pentest/anno, focalizzati su:
 - Perimetro esterno;
 - Applicazioni Web;
 - LAN dell'HQ;
 - Una LAN a campione presso una filiale;
 - Vettori di attacco proposti "liberamente" dai singoli vendor (ethical hacking)

Storie di vita vissuta – 2

- Azioni intraprese:
 - ◆ Stesura della RFQ.
 - **Metodologie e Best Practices** da utilizzare (**OSSTMM, OWASP**)
 - **Certificazioni obbligatorie** (e non): OPST, OPSA, CISSP, CISA, CISM
 - ◆ Selezione dei Fornitori.
 - Comprovata esperienza in realtà simili per tipologia e dimensionamento;
 - Policy di scouting per le aziende proponenti.
 - ◆ Definizione delle Regole di Ingaggio
 - ISECOM Rules of Engagement.
 - ◆ CV dei penetration tester
 - Policy di *ethical-scouting* per i Tiger Team proponenti.

Storie di vita vissuta – 3

- Commenti a quanto appena esposto:
 - ◆ OSSTMM, OWASP.
 - **La maggior parte** delle aziende proponenti **afferma** di utilizzare sia l'OSSTMM che l'OWASP (godetevi la prossima slide...)
 - **Certificazioni:** alcuni OPST, pochi OPSA, pochi CISSP, praticamente nessun CISA e CISM (!!!)
 - ◆ Comprovata esperienza: invio di “Sample Penetration Test reports”:
 - effettuati presso realtà non confacenti ai requisiti;
 - non “sanitizzati” (!!!)
 - eseguiti “*veramente male*”
 - *neanche lontanamente* “compliance” con l'OSSTMM
 - ◆ CV dei penetration tester
 - disclosure dettagliato dei security projects di N aziende !

Storie di vita vissuta – 4

- I primi problemi: esempio di un report inviato come “sample”

Introduzione

- L'attività di V.A. e P.T., condotta attenendosi a metodologie **OSTEM-oriented** ed in linea allo standard ISO 27001 (ISO 17799 compliant), si é articolata in 7 fasi:

- | | |
|--------------------------|---|
| 1. Enumerazione | Raccolta informazioni relative agli obiettivi. |
| 2. Scansione | Determinazione dei servizi erogati e da investigare. |
| 3. Ricerca vulnerabilità | Individuazione e valutazione dei fattori di rischio. |
| 4. Controllo puntuale | Controllo diretto delle vulnerabilità riscontrate. |
| 5. Attacco | Azioni controllate, mirate a violare:
confidenzialità , integrità , disponibilità. |
| 1. Sintesi | Documentazione schematica delle conclusioni raggiunte. |
| 2. Azioni correttive | Proposta piano di rientro. |

Storie di vita vissuta – 5

- I VERI problemi:
 - ◆ NESSUN fornitore ha proposto dei Vettori di Attacco **effettivamente utili** all'azienda Cliente.
 - ◆ Tiger Team members di dubbia etica, valori, esperienza;
 - ◆ Penetration Testers della società X, “passati” alla società Y, che subappaltava alla società Z..... ☹
 - E le vostre informazioni, attraverso quanti laptop, hard drives e revisioni di Word passeranno ?!?
 - ◆ Profili dei penetration tester: rilevate le cose *più assurde* in m.I. pubblici e non...
 - Richieste di aiuto su m.I., fornendo dettagli tecnici dell'infrastruttura dei Clienti;
 - Disclosure dei Clienti testati (con tanto di ragione sociale!!) nei pub alla sera....

Storie di vita vissuta – 6

- Lessons learned:
 - ◆ **Eccessiva** attenzione verso “quello che viene affermato, quello che è scritto”: esistono altri points of view!
 - ◆ “braccino corto” verso budget per vettori di attacco “non convenzionali”:
 - Incidents don't care about “legality”;
 - Incidents don't care about “legitimacy”;
 - Incidents don't care about “budgets”!
 - ◆ **Non sempre** l'azienda blasonata eccelle anche nelle nicche di mercato: spesso il grosso nome utilizza realtà aziendali molto più piccole. Perché **continuare** a pagare due volte ?!?

Errori tipici

Errori tipici - 1

- **Confusione nelle terminologie.**
 - Non mi stancherò mai di ripeterlo: un “V.A.” **non è** un “P.T.” !!!
- (conseguente) Chaos nel **confronto delle offerte** (e relativo budget a disposizione)
- **“il poco porta poco”**: se si paga poco un consulente, tendenzialmente si otterrà poco.
 - Il problema, però, torna ad essere quello della **riservatezza** dei dati;
 - Avete idea del **livello**, della **tipologia** e del **numero** di c.d. “informazioni sensibili” che emergono durante un penetration test...e che un pentester può acquisire ?
- Esempi recenti ?
 - “Business breaks security” approach: **LGT Lichtenstein, SocGen**
 - “Money breaks security” approach: **Ferrari, Telecom Italia**

Errori tipici - 2

Aspetti legali negli SLA: *

- **Definizione dello SLA**
- **Funzione dello SLA**
 - **Qualificare l'inadempimento dell'appaltatore;**
 - **Garantire la qualità del servizio;**
 - **Definire le aspettative delle parti;**
 - **Consentire all'appaltatore di allocare le risorse.**
- **Key Performance Indicators (RAVs dell'OSSTMM ?)**
- **Penali per violazione degli SLA**
- **Penali per ritardo**
- **Limitazioni/grace period**
- **Performance credits**
- **Benchmarking**
- **Recesso**

* Questi punti sono tratti dalla presentazione “L'acquisto di servizi IT: case study” degli Avv. Domenico Colella e Laura Liguori

Altre valutazioni

Attre valutazioni da fare *

- Riservatezza delle informazioni, degli output (reports, raw data, etc...)
- Trattamento dei dati personali
- Sub-appalto
- Clausole di prevalenza
- Distrazione del personale
- Controversie
- Cessione del contratto
- Altro...

* Questi punti sono tratti dalla presentazione “L’acquisto di servizi IT: case study” degli Avv. Domenico Colella e Laura Liguori

Conclusioni

Conclusioni

- Conoscenze tecniche.
- Elasticità, apertura mentale: essere realisti.
- Controllo della qualità degli output.
- Partecipazione dei referenti tecnici aziendali alla stesura degli SLA ed alla selezione dei Fornitori.
- Trasparenza su tutto il processo di verifica della sicurezza delle informazioni.

Riferimenti

Riferimenti

- Studio Legale Portolano Colella Cavallo (Roma): L'acquisto di servizi IT: case study. Milano, 27 maggio 2008.
www.portolano.it
- OSSTMM: www.osstmm.org
- OWASP: www.owasp.org
- ISECOM Rules of Engagement:
<http://www.isecom.org/projects/rules.shtml>

Q&A

- Grazie per l'attenzione !

DOMANDE ?

Raoul Chiesa

rchiesa@CLUSIT.it