

Associazione  
Informatici  
Professionisti

Osservatorio Privacy e  
Sicurezza delle  
Informazioni



# ***La Sicurezza Informatica come professione. Certificazioni, mondo del lavoro, prospettive***

***Paolo Giardini***

AIP Privacy Officer

Staff Backtrack Italia

Consiglio Direttivo GNU/LUG Perugia

Eucip Certified Informatics Professional

Centro di Competenza per l'Open Source

Consulente per la sicurezza delle informazioni

Direttore Osservatorio Nazionale Privacy e Sicurezza Informatica

Socio ILS - AIP - OPSI - AIPSI - CLUSIT - ISSA - BACKTRACK.IT

***Perugia, 2 dicembre 2009***

# About me



Mi occupo di:

- **Sicurezza** (Clusit, Aipsi, ISSA, OPSI, Sikurezza.org, Backtrack.it)
- **Privacy** (Direttore osservatorio Privacy e Sicurezza delle Informazioni)
- **Open Source** (CCOS, LUGPG, Italian Linux Society)
- ...ed altro :-)

<mailto:paolo.giardini@aipnet.it>  
<http://blog.solution.it>

# Sommario



## Sicurezza e mondo del lavoro

- Come le Aziende vedono la sicurezza informatica
- Hackers vs Security Professionals
- La sicurezza ed il mondo del lavoro
- Le certificazioni
- Il ruolo delle associazioni
- Question time

# La sicurezza in Azienda



Le aziende, specie le piccole e medie imprese ma in qualche caso anche aziende di grandi dimensioni non hanno una reale percezione del significato di “sicurezza informatica”.

I dati non vengono considerati come una risorsa da proteggere ma solo come “oggetti” da utilizzare non valutando il loro reale valore per l'azienda.

*Come vedono la sicurezza le aziende ?*

- Gli investimenti nella sicurezza sono solo un costo ulteriore.
- Gli obblighi di legge sono un inutile aggravio delle già tante incombenze amministrative.

*Alcune frasi famose:*

- “Tanto basta fare un po di documenti”.
- “Non abbiamo nulla che interessi un hacker”.
- “Abbiamo altre priorità”.

# Hacker ?

## *Cosa è un Hacker?*

### Definizione numero 1:

- Criminale informatico che entra nei computer e distrugge tutto e ruba i dati

### Definizione numero 2:

- Persona curiosa che si impegna nell'affrontare sfide intellettuali per aggirare o superare creativamente le limitazioni che gli vengono imposte

# Security Professionals



Il professionista di sicurezza informatica tutela la *disponibilità, riservatezza e integrità* del patrimonio di dati ed informazioni di aziende e istituzioni.

- Dispone di elevate conoscenze tecniche e capacità di calarsi nel problema
- Ha esperienza di Organizzazione Aziendale
- Conosce le normative Security Related
- Conosce ed applica Best Practice e Standard Internazionali
- Può avere una o più certificazioni

# Hackers vs Security Prof.



In realtà molti “Hacker” sono divenuti con il tempo affermati professionisti nel campo della sicurezza informatica, Da Kevin Mitnick a Raoul Chiesa

.. ma ovviamente non è indispensabile passare dal *Lato Oscuro della Forza* !

Anche se... **Black Hat Hackers**, **White Hat Hackers** e **Grey Hat Hackers** sono termini che indicano le molte sfaccettature dello stesso termine. Tanto che adesso si parla molto di **Ethical Hacking**

# Cosa cercano le aziende?



Molte aziende si attivano perché obbligate da norme p.e. Privacy (Dlgs 196/003), normativa bancaria (Basilea, MiFID, ecc.), responsabilità delle aziende (Dlgs.231/2001).

Altre vogliono evitare il ripetersi di eventi disastrosi (blocco attività a causa di virus, perdita di dati, furti di informazioni)

Sono poche sono le aziende che gestiscono le problematiche di sicurezza perché capiscono i rischi o perché lo ritengono un vantaggio competitivo

# Aree di attività



- Privacy
- Forensics
- Certificazione del codice
- Incident response
- Sicurezza industriale
- Business continuity
- Gestione dei rischi e compliance
- Analisi di sicurezza, pentesting, ecc.
- Certificazioni ISO ecc.
- Gestione documentale e Conservazione Sostitutiva
- Posta Elettronica Certificata e Firma digitale
- Pubblica amministrazione
- Infrastrutture critiche e NOS

# Cosa offre il mercato



Dai “praticoni” self made in grado a malapena di lanciare tool automatizzati (nmap, nessus, ecc.) a professionisti, certificati o meno, in grado di comprendere le esigenze aziendali e proporre il giusto equilibrio fra sicurezza e paranoia (anche se “*paranoia is a virtue*” - David A. Wheeler - Secure Programming for Linux and Unix HOWTO -1999)

Quale il giusto compromesso per l'azienda?

Essere in grado di rispondere a questa domanda può far emergere il Professionista serio e preparato

# Standard Internazionali



- BS7799 British Standard
- ISO 27000 series - ISMS Information Security Management System
- ISO 15408 - Common Criteria
- ISO/IEC 18028 - IT Network Security
- CoBIT - Control Objectives in IT
- NIST - National Institute of Standard and Technologies

NB: sono solo alcuni degli standard esistenti

# ISO 27001



- Provvede a fornire un modello per la creazione, l'implementazione, funzionamento, il monitoraggio, la verifica, il mantenimento e miglioramento di un **Information Security Management System (ISMS)**
- Derivata da BS7799-2 nel 2005
- Prevede l'impiego del modello PDCA (Plan - Do - Check - Act)
- E' il manuale per il conseguimento della certificazione

# ISO 27002



- Code of practice for information security
- Deriva dalla BS7799-1, poi ISO 17799 infine 27002 nel 2007
- Applica nella pratica i metodi stabiliti dalla 27001
  - Structure
  - Risk Assessment and Treatment
  - Security Policy
  - Organization of Information Security
  - Asset Management
  - Human Resources Security
  - Physical Security
  - Communications and Ops Management
  - Access Control
  - Information Systems Acquisition, Development, Maintenance
  - Information Security Incident management
  - Business Continuity
  - Compliance

Si dividono generalmente in **Vendor Neutral** e **Vendor Specific**.

Certificazioni Vendor Specific:

In larga parte strettamente legate al prodotto (Check Point, Symantec, SonicWall, Cisco, Microsoft, ...) trovano limiti nell'applicazione in ambienti eterogenei

# Principali certificazioni vendor neutral



- **(ISC)2** International Information Systems Security Certifications Consortium
  - CISSP Certified Information Systems Security Professional
  - SSCP System Security Certified Practitioner
- **ISACA** Information Systems Audit and Control Association
  - CISA Certified Information Systems Auditor
  - CISM Certified Information Security Manager
- **SANS** Institute
  - GSEC GIAC Security Essentials Certification
  - [...] (firewall, intrusion, forensics, consultant, windows, unix, auditor, ...)
  - GSE GIAC Security Expert
- **ISECOM** - Institute for Security and Open Methodologies
  - OPST OSSTMM Professional Security Tester
  - OPSA OSSTMM Professional Security Analyst
  - OPSE OSSTMM Professional Security Expert
- **CompTIA** Computing Technology Industry Association
  - CompTIA Security +
- **EUCIP** European Certification of Informatics Professionals
  - IT Administrator Modulo 5

# Il valore delle Certificazioni



Gli elementi che danno valore ad una certificazione sono essenzialmente:

- l'adeguamento continuo dei contenuti alle reali necessità del mercato
- l'autorevolezza e la serietà nella valutazione e nel rilascio della certificazione (alcune certificazioni prevedono adesione ad un codice etico, presentazione da parte di un soggetto già certificato, esperienza pregressa)
- il riconoscimento internazionale della certificazione

# Serve la Certificazione?



Dipende:

- Dal contesto aziendale (alcune aziende, Banche, Assicurazioni, ecc, necessitano di specialisti anche per obblighi contrattuali e normativi)
- Dalle aspettative del professionista (in molti ambienti la certificazione non è richiesta, in altri è punto di merito, in altri è indifferente)
- Dall'esperienza accumulata dal professionista (ho più volte visto personaggi “certificati” ma privi di esperienza trovarsi in difficoltà)

# Il ruolo delle Associazioni



La professione di informatico “non esiste”, non essendo regolamentata da un Ordine

Chiunque può progettare un sistema informatico. Non è così per un impianto elettrico o idraulico.

Le associazioni vogliono ottenere il riconoscimento giuridico al fine poter garantire ai consumatori i requisiti professionali dei propri iscritti (p.e. tramite la Formazione Continua)

E ora, a voi!



***Domande?***

Fine!



# *Grazie Dell'attenzione*

*<mailto:paolo.giardini@aipnet.it>*

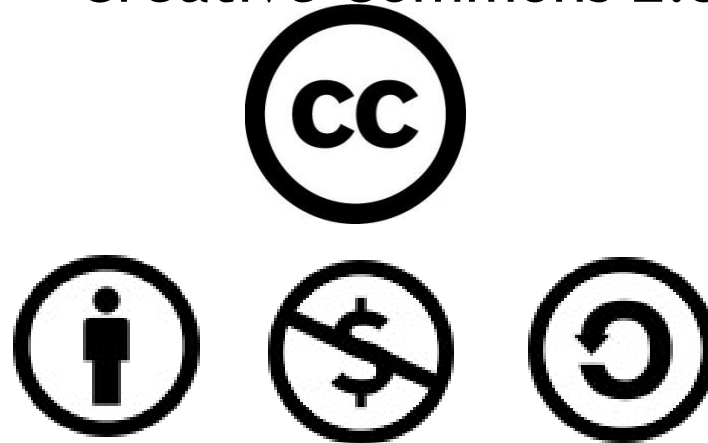
<http://blog.solution.it>

<http://www.aipnet.it>  
<http://www.aipsi.org>  
<http://www.clusit.it>  
<http://www.issa.org>  
<http://www.isecom.org/osstmm/>  
<http://www.isaca.org/>  
<http://www.isaca.org/cisa>  
<http://www.isaca.org/cism>  
<http://www.isc2.org/>  
<http://www.backtrack.it>  
<http://www.wardriving.it>  
<http://www.iso27001security.com/html/others.html>  
<http://www.iso27001security.com/>  
<http://it.wikipedia.org/wiki/Hacker>  
<http://www.autistici.org/hackarena/etica/jargon.htm>  
[http://www.auraweb.it/articolo\\_benessere.asp?cid=23&aid=1210](http://www.auraweb.it/articolo_benessere.asp?cid=23&aid=1210) (associazioni)  
<http://www.ifo.it/skills/DocumentiITA/STUDIO%20SULLE%20CERTIFICAZIONI%20ICT.doc>  
[http://www.clusit.it/download/Q02\\_web.pdf](http://www.clusit.it/download/Q02_web.pdf)

<http://catb.org/~esr/faqs/hacker-howto.html> How to become a Hacker – Steven Raymond

# Licenza d'uso

Questo lavoro viene distribuito sotto licenza  
Creative Commons 2.5



Sei libero di copiare, distribuire, trasmettere quest'opera e di modificarla a condizione di: attribuirne la paternità all'autore originale, non usare quest'opera per fini commerciali, condividerla allo stesso modo.