Mandato del gruppo Auditing INFN

Luglio 2010

Questo documento si propone di definire il mandato del gruppo Auditing INFN, istituito originariamente dalla Commissione Calcolo e Reti come un sottogruppo del gruppo Security.

L'attività di auditing interno è definita come:

> *Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.*[1]

E, in generale, ci si aspetta che gli auditor rispettino i principi di[2]:

- integrità,
- obiettività,
- confidenzialità.

Il gruppo di Auditing INFN si occupa esclusivamente di sicurezza informatica e nasce in attuazione a quanto stabilito dalla direttiva del 16/1/2002, pubblicata nella Gazzetta Ufficiale n. 69 del 22 marzo 2002, recante raccomandazioni per la "Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni" e recepita dall'Ente con l'adozione della Carta della Sicurezza Informatica (C.D. 23/2/2007).

L'obiettivo dell'auditing INFN, come sopra specificato, si concretizza sia nell'effettuazione di indagini strutturate e periodiche allo scopo di rilevare eventuali vulnerabilità, configurazioni non corrette, il mancato rispetto di normative e leggi specifiche o la non aderenza alle politiche di sicurezza adottate dall'Ente, sia in azioni di supporto nell'indicare possibili soluzioni e nel fornire strumenti per il self-auditing delle sedi.

Le attività previste possono essere riassunte nei punti seguenti:

- raccolta di informazioni sull'organizzazione delle risorse informatiche;
- analisi dei rischi per individuare le priorità delle attività da svolgere;
- analisi delle politiche di sicurezza adottate;
- rilevazione dei servizi ritenuti "pericolosi", esposti all'esterno delle varie reti locali;
- ricerca di vulnerabilità e verifica delle configurazioni dei server individuati nel punto precedente;
- verifica della configurazione delle apparecchiature di rete (*router*, *switch*, ecc.);
- emissione di raccomandazioni per ovviare alle vulnerabilità rilevate e verifica della loro applicazione;

1 Information Systems Audit and Control Association (ISACA), www.isaca.org

2 The Institute of Internal Auditors, *Code of Ethics*, http://www.theiia.org/guidance/standards-and-guidance/ippf/code-of-ethics/english/

- stesura di rapporti periodici, destinati ai responsabili locali e alla Direzione dell'Ente.

Altre attività, quali ad esempio la verifica dell'applicazione dei Documenti Programmatici sulla Sicurezza, verranno aggiunte quando le risorse umane a disposizione del gruppo lo consentiranno.

Il gruppo cercherà di uniformarsi, per quanto possibile, agli standard e alle *best practice* in vigore e, a questo proposito, si segnala la necessità per i suoi membri di seguire corsi periodici di aggiornamento

Più specificamente, i controlli da remoto che verranno eseguiti saranno i seguenti:

- scansioni *continue* con **nmap** (o equivalente) su tutte le macchine *con indirizzi gestiti dall'Ente*, inclusi switch e router, per la rilevazione di servizi accessibili dall'esterno delle reti locali;
- scansioni periodiche con **nessus** (o equivalente) sulle macchine individuate nel punto precedente alla ricerca di eventuali vulnerabilità: queste attività, a differenza delle precedenti, verranno preannunciate.

Modifiche ed ampliamenti a questa lista, come pure altri tipi di verifiche – quali ad esempio la sensibilità ad attacchi di tipo *social engineering* – verranno preventivamente discussi con la Commissione Calcolo e Reti.

Sarà cura del gruppo svolgere le attività di cui sopra, in particolare le scansioni alla ricerca di vulnerabilità, nel modo più "leggero" possibile e con un ampio preavviso. E' chiaro, però, che si tratta di azioni inerentemente intrusive e che quindi potranno provocare interruzioni dei servizi in esame, crash di macchine e altri malfunzionamenti, di cui il gruppo non potrà essere ritenuto responsabile. Sarà ovviamente sempre possibile, su richiesta del responsabile, escludere macchine particolarmente critiche.

Dopo ogni ciclo di verifiche, le segnalazioni delle nuove vulnerabilità rilevate saranno inviate ai responsabili indicati delle varie Strutture perché possano prendere le opportune contromisure. Il gruppo produrrà inoltre un rapporto, almeno annuale, delle sue attività e dei suggerimenti da presentare alla Direzione dell'Ente.