Audit di Sicurezza

Matteo Boschini, Enrico Cavalli
CILEA, Segrate

Abstract
Il CILEA propone un nuovo servizio di Audit di Sicurezza ispirato alle norme ISO 27001 e ISECOM OSSTMM.

CILEA presents its new Security Audit Service which follows ISO 27001 and ISECOM OSSTMM templates.

Keywords: Security Audit, ISO 27001, ISECOM, OSSTMM.

Introduzione

Sempre più aziende ed enti pubblici sono sensibili alle problematiche della sicurezza informatica e, più in generale, delle informazioni. Un notevole impulso in questo senso è stato dato dall'impianto normativo sulla tutela della privacy, il famoso Decreto Legislativo 196/03, in materia di trattamento dei dati personali. Inoltre, molte aziende sono rimaste "scottate", dal punto di vista della sicurezza, per vari motivi: dal banale virus, alla perdita di dati preziosi perché il sistema di backup non sempre è efficace, e così via.

Ormai si danno per scontate tecnologie per la sicurezza perimetrale (firewall, VPN), tecnologie più o meno reattive contro le intrusioni (Intrusion Detection System, Intrusion Protection System), metodi di autenticazione forti (es. smartcard).

Anche in realtà medio piccole è ormai tangibile una visione della sicurezza fatta non soltanto da prodotti tecnologici che si acquistano, si installano e si dimenticano, ma anche da un importante contorno di gestione e di procedure che deve far funzionare le singole tecnologie in un contesto unificato, commisurato alle proprie specifiche esigenze.

Di fatto, è quindi arrivato il momento di verificare con uno sguardo non solo tecnicistico quanto efficaci siano le misure di sicurezza adottate.

L'audit di sicurezza

In questo contesto si inserisce il Security Audit proposto dal CILEA. Lo scopo è quello di fare una fotografia delle misure di sicurezza implementate dal cliente che lo richieda, cercando di evidenziare eventuali mancanze o vulnerabilità.

Se è vero che diverse verifiche che presentiamo nel seguito possono essere effettuate "in proprio", è altrettanto importante ricordare che farle effettuare a una parte indipendente, garantisce il requisito di separazione dei ruoli sancito in ogni contesto di Audit.

L'analisi riguarda sia gli aspetti di gestione della sicurezza, basandosi sullo standard internazionale ISO 27001, sia gli aspetti tecnici, basandosi sulla procedura ISECOM OSSTMM2.2.

L'Audit di Sicurezza parte da un'analisi a tavolino dell'infrastruttura del cliente, verificando quali dei controlli obbligatori della norma ISO 27001 siano stati applicati.

In particolare, le macro aree di indagine coperte da questa fase riguardano principalmente:
- *security policy* (e quindi il DPS – Documento Programmatico sulla Sicurezza);
- sicurezza nei rapporti con i fornitori;
- sicurezza relativa alle risorse umane;
- sicurezza fisica e ambientale;
- *business continuity* e *disaster recovery*;
- sicurezza di rete;
- controllo degli accessi;
- gestione del ciclo di vita dei sistemi informativi (sviluppo, test, *deploy*, dismissione);
- gestione degli incidenti;
- conformità rispetto alla normativa vigente.

A corollario viene effettuata anche un'indagine a campione per verificare il livello di sensibilizzazione degli utenti finali circa le problematiche relative alla sicurezza (ricordiamo che

la normativa sulla privacy prevede l'istituzione di percorsi formativi per rendere edotti gli incaricati circa i rischi che incombono su dati personali e sensibili). Terminata questa prima fase, si passa a investigare la struttura tecnica, cercando eventuali vulnerabilità, sia con strumenti automatizzati che con un processo manuale. Naturalmente l'analisi verrà effettuata sia dall'interno della rete del cliente, che dall'esterno (in un secondo momento). A seconda della natura e della dimensione delle infrastrutture del cliente, l'analisi potrà essere esaustiva, oppure condotta a campione. La profondità e il dettaglio dell'analisi vengono sempre concordati con il cliente, tenendo ben distinti il semplice *vulnerabiliy assessment* dal *penetration test*. Nel primo caso si verifica soltanto l'esistenza di vulnerabilità, mentre nel secondo si prova a sfruttarle.

Vale la pena ricordare che il fatto che non vengano evidenziate vulnerabilità, o che non si riesca a sfruttare eventuali vulnerabilità, non implica automaticamente che non esistano affatto vulnerabilità (sfruttabili) nella struttura del cliente nel momento di esecuzione dei test o in futuro.

Tra gli aspetti che vengono verificati ricordiamo i seguenti:

- configurazione e robustezza di LAN e WAN;
- livello di sicurezza dei singoli server rispetto agli aggiornamenti del produttore e a corretta configurazione;
- regole di firewall (ed eventualmente IDS) – ingress/egress filtering, IP spoof;
- strumenti di autenticazione e autorizzazione;
- vulnerabilità di applicativi WEB (*information disclosure, cross site scripting, SQL injection*).

Al termine dell'analisi, al cliente viene consegnato un rapporto diviso in executive summary e in raccomandazioni tecniche. Il cliente riceve quindi una serie di raccomandazioni per migliorare la gestione della propria sicurezza, a sostegno delle quali vengono comunque sempre prodotte tutte le evidenze riscontrate in fase di Audit.

A questo proposito, vale quindi la pena di ricordare che l'Audit di Sicurezza non equivale a una certificazione ISO 27001, bensì potrebbe essere parte di un percorso volto alla certificazione stessa. Visto che la sicurezza è da intendersi come un processo di continuo miglioramento, l'Audit diventa un indispensabile momento di verifica delle soluzioni implementate. Ripetere l'Audit a scadenze regolari consente di tenere monitorati, in maniera indipendente, gli avanzamenti in questo processo virtuoso.