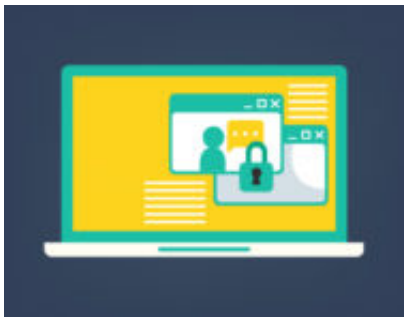
Sviluppo sicuro delle applicazioni: i test di sicurezza

Date : 8 febbraio 2018



Questo articolo prosegue la serie dedicata a temi su cui ci sono i maggiori dubbi e perplessità sulle norme della serie ISO/IEC 27000.

In due articoli precedenti si è trattato del processo di sviluppo e dei requisiti di sicurezza. Questo è dedicato ai test.

Sui test di sicurezza in ambito applicativo è disponibile molta letteratura, a cui si rimanda. Dopo un paragrafo per inquadrare la questione e presentare la terminologia qui usata, sono affrontati alcuni aspetti.

Cosa sono i test di sicurezza (vulnerability assessment)

I *vulnerability assessment* sono delle analisi e valutazioni delle potenziali vulnerabilità di un sistema informatico.

Essi possono essere condotti in molti modi, tra cui:

- riesame dei requisiti funzionali e delle specifiche tecniche del sistema informatico basandosi sulla documentazione disponibile;
- riesame del codice sorgente delle applicazioni (*code review)*;
- verifica della qualità e sicurezza del codice statico (SAST o Static application security testing);
- verifica della qualità e sicurezza del codice dinamico (DAST o Dinamic application security testing);
- scansione automatica dei sistemi informatici con strumenti di *vulnerability scanning*;
- prove di attacco da parte di personale specializzato (*penetration testing*); a sua volta, il *penetration test* può essere condotto da persone senza conoscenze del sistema da analizzare (test *black box*) o con piena conoscenza del sistema (test *white box)*.

Test specializzati possono essere condotti concentrandosi sulle vulnerabilità che potrebbero essere sfruttate per condurre attacchi dall'interno o dall'esterno della rete in cui è attestato il sistema (da ricordare che un attacco dall'interno può essere condotto dal personale interno o

da esterni che sfruttano un sistema interno già compromesso in precedenza).

Chi conduce i test di sicurezza è designato con diversi termini (*ethical hacker, white hat*). Si può usare anche il termine più prosaico di *valutatore*.

I test di sicurezza possono essere condotti da personale interno o da fornitori. Nel caso di fornitori è sempre necessario stipulare un contratto per stabilire le responsabilità reciproche e i limiti dei test (per esempio, i valutatori si impegnano a non condurre attacchi che possano compromettere i sistemi, ma a spingere l'analisi solo per dimostrare la presenza e l'utilizzabilità, da parte di un malintenzionato, delle vulnerabilità).

In questo articolo ci concentriamo sui test dei sistemi informatici, ma gli stessi principi possono essere applicati alle verifiche della sicurezza fisica (per verificare se un malintenzionato può accedere ad aree senza avere le necessarie autorizzazioni) e della consapevolezza del personale (per verificare le potenzialità di successo di un attacco di *social engineering*).

Non solo scansioni o penetration test

Da anni le società specializzate in sicurezza mettono l'accento sull'importanza dei *vulnerability assessment*, intesi solo come *vulnerability scanning* e *penetration test* in ambienti di pre-produzione o produzione. Questa visione è stata accolta anche dai normatori che troppo spesso richiedono di condurre scansioni di sicurezza senza accompagnare questo requisito con altri di tipo più preventivo.

Chiunque si occupa di sicurezza conosce il principio del *security-by-design* (ripreso nell'ambito della protezione dei dati personali come *privacy-by-design*): la sicurezza deve essere considerata e progettata fin dalle prime fasi dell'analisi e dello sviluppo dei sistemi informatici. Grazie al GDPR questo approccio sta diventando sempre più noto.

Per questo motivo è sbagliato concentrare l'analisi della sicurezza solo nella fase finale di test. È quindi giusto ricordare l'importanza di *vulnerability scanning* e *penetration test,* ma senza dimenticare le altre tecniche.

Quando condurre test sulla sicurezza

I test sulla sicurezza vanno condotti lungo tutto il ciclo di vita del sistema informatico.

In fase di progettazione e sviluppo, i test possono essere condotti sulla documentazione prodotta per verificare la completezza e coerenza delle funzioni e dei meccanismi tecnologici per la sicurezza; durante tutto lo sviluppo va verificata la qualità e sicurezza del codice e la correttezza delle integrazioni; in pre-produzione vanno condotte scansioni complete del sistema.

Prima di portare un sistema in ambiente di produzione, esso dovrebbe essere verificato anche con *penetration test.*

I test vanno condotti anche a seguito di cambiamenti significativi con potenziali impatti alle funzioni e ai meccanismi di sicurezza, sempre in ambiente di pre-produzione (infatti i test in ambiente di produzione potrebbero avere degli impatti sulla produzione stessa, inoltre non bisognerebbe mai promuovere un sistema in ambiente di produzione senza prima essere sicuri della sua sicurezza).

Anche se il sistema non è modificato, andrebbero condotti test periodici sulla sua sicurezza. Infatti nuove vulnerabilità potrebbero essere emerse o nuove tecniche di attacco potrebbero essere disponibili.

Perché coinvolgere persone specializzate?

A rigore non ci dovrebbe essere necessità di coinvolgere persone specializzate (o società esterne) per condurre i test di sicurezza: gli analisti, gli sviluppatori e tutto il personale addetto alla progettazione e sviluppo dei sistemi dovrebbero essere sufficientemente competenti per prevenire vulnerabilità e produrre un sistema sicuro.

Nella realtà, gli sviluppatori si concentrano sulle funzionalità per gli utenti; questo inevitabilmente a discapito di quelle di sicurezza. Per questo è necessario coinvolgere nei progetti persone che invece hanno sviluppato queste ultime competenze e concentrano il proprio lavoro su di esse.

Questo non toglie che gli sviluppatori dovrebbero avere elevate competenze in materia di sicurezza: non è pensabile si possa produrre un buon sistema se questo è stato oggetto di continue modifiche a seguito delle segnalazioni da parte degli esperti di sicurezza. Ancora una volta, la sicurezza dovrebbe essere considerata sin dall’inizio, e questo può essere fatto solo con il pieno coinvolgimento degli sviluppatori.

Il programma dei test

È sempre necessario predisporre un *programma dei test*. Questo dovrebbe riportare tutti i sistemi e tutti i possibili test, per poi selezionare quali condurre in un certo periodo di tempo, quali posticipare, quali non condurre. Per ciascun test va stabilita la frequenza.

In realtà di medie o grandi dimensioni non è immaginabile si possano verificare tutti i sistemi con tutte le tecniche possibili. Questo non solo per questione di costi (che potrebbero anche rivelarsi insostenibili), ma perché sarebbe necessario bloccare il personale per lunghi periodi di tempo per seguire i test e, successivamente, realizzare le opportune correzioni.

Il programma dei test è quindi utile per assicurare la completezza e significatività dei test, ossia per dimostrare che, in un certo periodo di tempo, tutti i test necessari sono condotti sui sistemi che li necessitano. Alcuni programmi sono strutturati su un arco di tempo di 3 o 5 anni.

Il programma dei test deve considerare la disponibilità di tempo delle persone che li conducono e deve anche lasciare spazio per test straordinari (per esempio, a seguito di modifiche

significative ai sistemi più critici).

A cura di: **Cesare Gallotti**