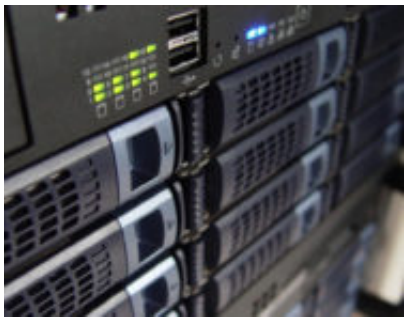
Inventario degli asset: l’incompreso

Date : 16 giugno 2017



Questo è il primo di una serie di articoli di approfondimento relativi ad elementi di un sistema di gestione per la sicurezza delle informazioni. Saranno dedicati a temi su cui ci sono i maggiori dubbi e perplessità sulle norme della serie ISO/IEC 27000.

Il primo tema, oggetto di questo articolo, è l’inventario degli asset, dichiarato da auditor e consulenti come importantissimo, ma spesso visto come inutile e faticoso da parte dei tecnici.

Nell’ambito della gestione dei servizi IT, l’inventario degli asset, con qualche requisito in più, prende il nome di *configuration management database* (CMDB) o *configuration management system* (*CMS*). In quell’ambito, l’inventario prevede anche che siano presenti le relazioni tra i servizi e gli asset (o *configuration item*) necessari alla loro erogazione.

L’inventario degli asset serve a conoscere e controllare gli elementi di un sistema di gestione per la sicurezza delle informazioni. Tra questi elementi ci sono i server, i pc, i dispositivi di uso personale, i dispositivi di rete, le sedi, gli impianti di sicurezza, gli archivi fisici, le informazioni stesse e il personale. Altri, come i redattori della ISO/IEC 27005, introducono anche i processi.

Purtroppo non è facile capire come organizzare un inventario di tutti questi elementi in modo che sia utile e non eccessivamente faticoso da mantenere.

Si ricorda che un meccanismo di sicurezza inefficiente, poi viene mantenuto male e diventa inefficace. Questo poi può essere dannoso, in quanto un uso scorretto di un meccanismo di sicurezza può introdurre delle vulnerabilità.

Come deve essere

L’inventario degli asset non deve essere visto come unica entità: non sarebbe una soluzione intelligente elencare sistemi informatici, impianti di sicurezza e persone in un unico documento. Infatti i sistemi informatici sono governati dagli informatici, gli impianti di sicurezza da chi si occupa di sicurezza fisica e le persone da altre funzioni.

Un inventario degli asset deve riportare le informazioni utili per monitorare e mantenere ciascun

asset.

Propongo qui di seguito un esempio non esaustivo di inventari e di informazioni necessarie:

1. le applicazioni, i server e i dispositivi di rete sono facilmente monitorabili con sistemi di controllo della rete; il loro inventario è quindi on-line; è opportuno fare in modo che i sistemi siano denominati e raggruppati in modo da avere velocemente chiaro il loro utilizzo (per esempio, è meglio non nominare il file server solo con una sigla C10-192-44, ma anche con un suffisso “file-server”) e i loro utilizzatori; devono essere raccolti i dati necessari all’assistenza (per esempio, ubicazione, sistema operativo, indirizzo IP o sottorete);
2. i dispositivi in uso al personale dovrebbero essere elencati con marca e numero di serie, sistemi operativi, indirizzi IP se fissi, nome del sistema e assegnatario; nelle PMI è sufficiente un file, mentre in quelle più grandi dovrebbe essere usato un database;
3. le sedi e gli archivi dovrebbero essere elencati insieme alle chiavi meccaniche in uso; si dovrebbero quindi elencare le chiavi e i loro assegnatari (per ogni chiave, almeno una copia dovrebbe essere assegnata al responsabile della sicurezza fisica della sede);
4. gli impianti di sicurezza dovrebbero essere elencati da chi si occupa di manutenzione; solitamente questi archivia in un faldone i manuali e i rapporti di installazione e manutenzione di ciascun impianto; dovrebbe essere anche mantenuto un elenco degli stessi impianti insieme ai riferimenti delle ditte specializzate da contattare in caso di necessità e le scadenze delle manutenzioni programmate;
5. le persone sono solitamente elencate dall’ufficio Personale o dall’ufficio Acquisti (nel caso di consulenti); sono anche censite dagli informatici quando utenti dei sistemi IT;
6. le informazioni possono essere tracciate in una tabella con indicate, per ciascuna area aziendale, le tipologie di informazioni trattate; questo compito può essere svolto insieme alla redazione del “Registro dei trattamenti” richiesto dal GDPR.

Come usarlo

Il primo utilizzo di un inventario degli asset è di tipo operativo. Un inventario degli asset è utile nelle seguenti occasioni:

- un sistema informatico non funziona e bisogna sapere velocemente di quale sistema si tratta e quali sono i servizi e le persone impattate, in modo da stabilire le priorità di intervento e le persone più adatte a intervenire;
- per ogni modifica ad un sistema è necessario valutarne le dipendenze e i potenziali impatti sugli altri sistemi e gli utenti;
- in occasione dell’entrata e dell’uscita del personale è necessario consegnare e ritirare le autorizzazioni e i dispositivi assegnati;
- quando una chiave meccanica si rompe è necessario predisporre dei duplicati o, se è necessario cambiare le serrature, fornire alle persone interessate una copia della nuova chiave;
- va tenuto aggiornato uno scadenziario delle manutenzioni programmate e devono essere prontamente rintracciabili i tecnici specializzati quando si guastano gli impianti di

sicurezza;
- vanno gestiti gli utenti dei sistemi informatici per assicurarne l’autenticazione e l’attribuzione delle autorizzazioni;
- vanno censite le persone in sede, in modo da controllare lo stato di eventuali evacuazioni.

Per quanto riguarda i sistemi informatici, è possibile usare un inventario da interfacciare ad un sistema di monitoraggio della rete in modo da rilevare nuovi dispositivi collegati.

Un’altra finalità di un inventario degli asset è l’attribuzione di un livello di criticità ai sistemi informatici e agli archivi, in modo da stabilire diversi livelli di sicurezza da garantire. Si intuisce sin da subito che un inventario usato per queste finalità deve essere di un livello di dettaglio molto inferiore a quello usato per finalità operative: può essere sufficiente uno schema di rete e un elenco dei servizi informatici presenti in ciascuna sottorete.

Infine un inventario degli asset può essere usato per la valutazione del rischio relativo alla sicurezza delle informazioni. In questo caso si dovrebbe usare un elenco poco dettagliato. È noto infatti che un aumento del dettaglio non migliora i risultati dell’analisi; ne allunga solo i tempi e richiede un maggiore impegno da parte dei partecipanti, con conseguente dispersione di energie in attività non necessarie e perdita di vista dell’obiettivo. La valutazione del rischio si basa su considerazioni soggettive e con prospettiva al medio-lungo termine e quindi non necessita di un elevato livello di dettaglio.

Mantenere un inventario

Deve essere stabilito un processo per cui ad ogni variazione degli asset (inserimento, modifica e ritiro) siano modificati gli inventari pertinenti.

Uno strumento troppo sofisticato e inefficiente da mantenere dopo poco non viene più usato in modo efficace e diventa quindi inutile.

Conclusioni

È necessario, in fase di progettazione di un inventario degli asset, considerarne la finalità e le risorse necessarie per mantenerlo. Spesso quindi è opportuno evitare di prevedere l’inserimento di dettagli che idealmente sono utili ma difficili da aggiornare, oppure prevedere degli inventari troppo dettagliati per le loro finalità.

Un inventario degli asset non deve rispondere alle necessità di un auditor o di un consulente, ma dell’organizzazione che deve mantenerlo e agli obiettivi che si è fissata.

A cura di: **Cesare Gallotti**