Valutazione dei rischi per la sicurezza delle informazioni: sicuri della soluzione adottata?

Risk assessment for information security: are you sure about the adopted solution?

Fabrizio Cirilli ♦

♦*PDCA Srl*

Sommario

Strumenti di ogni tipo sono utilizzati da migliaia di aziende ma non sempre è chiaro se e come funzionino certi strumenti informatici rispetto alla sicurezza delle informazioni.

Abstract

Tools of all kinds are used by thousands of companies but it is not always clear if and how certain IT tools work with respect to information security.

Durante gli audit di terza parte per la ISO/IEC 27001 ci si imbatte continuamente nelle valutazioni dei rischi basate su minacce-vulnerabilità di asset tecnologici.
Cerchiamo di capire se questa soluzione sia o no in linea con la ISO/IEC 27001 e se sia, in qualche modo, richiesta dalla norma o una scelta delle aziende e, in quest'ultimo caso, se paga o meno.
Iniziamo con dire che la ISO/IEC 27001 riguarda la sola sicurezza delle informazioni, si occupa cioè della riservatezza, integrità e disponibilità delle informazioni. Fatta questa premessa entriamo nella norma e verifichiamo dove e come questa cosa è fissata.
A proposito della valutazione dei rischi al requisito 6.1.2.c.1 troviamo:
applicando il processo di valutazione del rischio relativo alla sicurezza delle informazioni per identificare i rischi associati alla perdita di riservatezza, di integrità e di disponibilità delle informazioni incluse nel campo di applicazione del sistema di gestione per la sicurezza delle informazioni;
Siamo quindi certi che la norma non tratta di apparati connessi, almeno per quanto concerne la valutazione dei rischi inerenti alle informazioni. In questo tralasciamo le ovvie considerazioni tra le informazioni e gli asset tecnologici che le gestiscono, ci torneremo più tardi.
Non sono citate minacce o vulnerabilità per determinare i rischi nella ISO/IEC 27001.
E allora da dove spuntano queste due? Dalla ISO/IEC 27005 che non è una norma ma un documento a supporto per quelle organizzazioni che non hanno esperienza specifica sul tema.
La ISO/IEC 27005 specifica però che:

minacce e vulnerabilità non sono più richieste dalla ISO/IEC 27001
a partire dalla versione 2013; a tal proposito occorre precisare che l'attuale versione nazionale della norma del 2017 non modifica la versione originale.
Quindi non abbiamo ancora capito il perché minacce e vulnerabilità siano presenti in alcune valutazioni dei rischi delle aziende. Un'altra spiegazione possibile è che siano stati utilizzati dei tool o delle metodologie che ne fanno ancora uso. Spesso è così infatti.
Cosa fare? Niente, se funziona. Altrimenti basta tornare alla norma.
Una delle modifiche fondamentali del 2013 alla ISO/IEC 27001 è stata proprio quella di cercare di staccare la sicurezza delle informazioni dalla sicurezza informatica. È inevitabile parlando di minacce e vulnerabilità associare queste due chiavi di lettura agli apparati, dimenticando l'informazione che invece deve essere il centro della valutazione.
Perché continuare a parlare di rischi se ho le soluzioni tecnologiche più evolute? Perché dovrei spendere ulteriori risorse per incrementare i livelli di sicurezza dopo aver speso una montagna di denaro? Queste sono due delle domande più comuni che gli amministratori delle aziende si pongono in questi casi. Dal loro punto di vista è perfettamente logico: se ho la soluzione più evoluta i rischi dovrebbero essere gestiti.
Purtroppo, non è così perché gli apparati si concentrano su alcune dimensioni della sicurezza informatica ma non gestiscono altre parti tipiche della sicurezza delle informazioni (ad es. le competenze e la consapevolezza del personale, l'organizzazione aziendale, l'integrazione con i processi aziendali, il coinvolgimento del top management ecc.). Questi argomenti sono coperti dalla sicurezza delle informazioni, in un processo top down e non bottom up come nella sicurezza informatica.
Nella sicurezza informatica sono i tecnici, l'ICT a fare considerazioni, analisi, scegliere contromisure ecc. Nella sicurezza delle informazioni sono i risk owner. Ma chi sono i risk owner?
Per risk owner si intende quella *persona o entità che ha l'accountability e l'autorità per gestire i rischi*, non degli apparati ma i *rischi per le informazioni incluse nel campo di applicazione*.
Ora la domanda diventa: chi nella mia organizzazione ha autorità e accountability (è intraducibile quindi lo lasciamo come è nella norma)? Temo che la risposta si trovi nei vertici aziendali.
Non parliamo del Data Owner o del Process Owner, sono altre funzioni. Non è detto nemmeno che queste figure possano coincidere con i Risk Owner.
Quindi cosa devo fare? Ripensare al campo di applicazione e al contesto per identificare quali informazioni vanno protette e perché. Poi possiamo porci le domande: quali impatti avrei se perdessi la riservatezza di ogni informazione protetta? E se perdessi l'integrità? E se perdessi la disponibilità?
Non necessariamente gli impatti sono gli stessi; ad esempio, perdendo la riservatezza di dati personali (sempre che questi siano inclusi nel campo di applicazione) è chiaro il riferimento alle conseguenze in termini di GDPR e Privacy. Lo stesso vale per le penali nei contratti, per le sanzioni dovute a direttive e regolamenti applicabili alle informazioni nel campo di applicazione.

Quindi, più che un'analisi di minacce e vulnerabilità, qui si tratta di analizzare sanzioni, penali ecc. includendo danni di immagine e simili. Stiamo parlando di valutazioni di alto livello, indipendenti dagli apparati.
Altro discorso è quello della determinazione della *verosimiglianza realistica* (così è definita, non probabilità che riporterebbe a considerazioni di altra natura e fonte). Quanto è verosimile (possibile) che io possa perdere la riservatezza di una determinata informazione? E l'integrità? E la disponibilità?
Anche qui poco abbiamo a che fare con gli apparati, siamo piuttosto nel campo dei dati storici dell'azienda, delle informazioni esperienziali o della letteratura in materia. E di nuovo ad un livello alto che prescinde da minacce e vulnerabilità.
In definitiva, per ogni informazione inserita nel campo di applicazione del Sistema di Gestione per la Sicurezza delle Informazioni si devono determinare i rischi per la perdita di riservatezza, integrità e disponibilità delle informazioni e non degli apparati in quanto tali.
La formula per il calcolo del rischio è semplice:

$$R = I \times P$$

Dove I è l'impatto e P è la possibilità di accadimento (leggendola come RIP è mnemonicamente più facile e in qualche modo riconduce alle potenziali conseguenze per la mancanza di gestione del rischio). La formula va ripetuta per riservatezza, integrità e disponibilità per tutte le informazioni incluse nel campo di applicazione.
Posso fare una valutazione aggregata in termini di riservatezza, integrità e disponibilità delle informazioni? È poco efficace per il corretto dimensionamento del rischio ma possibile, specie nei tentativi iniziali può dare un'idea macroscopica del tutto. Poi però diventerà inefficace per la scelta delle contromisure da applicare.
Contromisure, questo era il termine originale e più consono, poi per un inglesismo siamo passati ai controlli, anche se il termine controllo tende a confondersi in italiano con un sostantivo che poco ha a che fare con il termine contromisura. Anche qui avremmo bisogno di qualche pagina per spiegare il caos che un termine improprio può generare per i non addetti ai lavori!
Torniamo alla valutazione dei rischi, c'è un altro punto che merita attenzione, il requisito 6.1.2.b:
assicuri <u>che ripetute</u> valutazioni del rischio relativo alla sicurezza delle informazioni producano risultati coerenti, validi e confrontabili tra loro
La parola magica è: "ripetute", quindi più di una! Considerando che quanto descritto nella norma avviene all'interno del ciclo PDCA, la valutazione dei rischi deve essere ripetuta (quindi almeno 2 volte) all'interno di ciascun ciclo PDCA. Ciò per assicurare *risultati coerenti, validi e confrontabili tra loro.*
Questo perché la prima valutazione mi misura, la seconda mi permette di capire se i trattamenti posti in atto hanno dato i loro effetti e se la valutazione dei rischi si sia effettivamente modificata come atteso.
Per dirla in modo semplice: mi peso prima della dieta, faccio la dieta (le mie contromisure) e poi mi ripeso per vedere se la dieta funziona o no come atteso.

Sembra un concetto facile ma implica una serie di considerazioni importanti che spesso sfuggono alle organizzazioni.
Non abbiamo dimenticato i nostri termini iniziali: minacce e vulnerabilità. Diciamo che anche l'ordine non è del tutto corretto. Se parliamo di asset informatici l'elemento primario è la vulnerabilità che potrebbe essere sfruttata da una minaccia per concretizzare un rischio.
Una chiave non è di per sé una minaccia, almeno fin quando non incontra la serratura adatta. Non posso dire che le chiavi costituiscano in senso assoluto una minaccia se non ho una porta dotata di serratura.
Quindi, le valutazioni dei rischi dovrebbero partire dalle vulnerabilità degli asset coinvolti (ma siamo di nuovo nel campo della sicurezza informatica). Infatti, una piattaforma come CVE (https://cve.mitre.org/) ha proprio questo compito: aiutare a comprendere quali vulnerabilità note sono collegate ai miei asset. Dopo potrò fare riflessioni sulle minacce in grado di sfruttarle. Spesso in audit emergono vulnerabilità come Spectre e Meltdown, è facile immaginare le considerazioni in merito a minacce e contromisure applicabili al caso.
Un altro punto per considerare il giusto ordine di analisi è lo "0day". Partiamo dalle vulnerabilità note, quando una minaccia riesce a sfruttare la vulnerabilità il gioco è fatto. Ora dovrebbe essere più chiaro il rapporto tra vulnerabilità, minacce e informazioni.
Allora perché il 90% di queste valutazioni parte dalle minacce? È come dire che siccome il furto esiste lo si applica a tutti gli asset aziendali. Bene, proviamo: il building? Il generatore elettrico? Gli UPS? Il sistema di condizionamento? Il NAS? Il Cloud!?
Qualcosa non torna. Probabilmente si parte dalle minacce perché sono l'argomento percepito dalle persone coinvolte nelle interviste. In questo caso è come chiedere una qualsiasi opinione alle persone, senza alcuna base di partenza. Ciò potrebbe causare alcuni effetti:

1. il risultato della valutazione conduce a un rischio *percepito,* che non necessariamente è correlato alle vere vulnerabilità;
2. sullo stesso asset, persone con esperienza diversa, potrebbero avere visioni diametralmente opposte, ampliando la scala del rischio a valori pressoché infiniti;
3. essendo tutto basato sulle minacce, se una minaccia non ha fondamento mi troverò ad avviare contromisure inutili, disperdendo soldi ed energie.

Per gli interessati recupero questo schema, tratto dalla ISO/IEC 13335 (lontana parente della sicurezza delle informazioni ritirata nel 2005, all'uscita della prima edizione della ISO/IEC 27001):

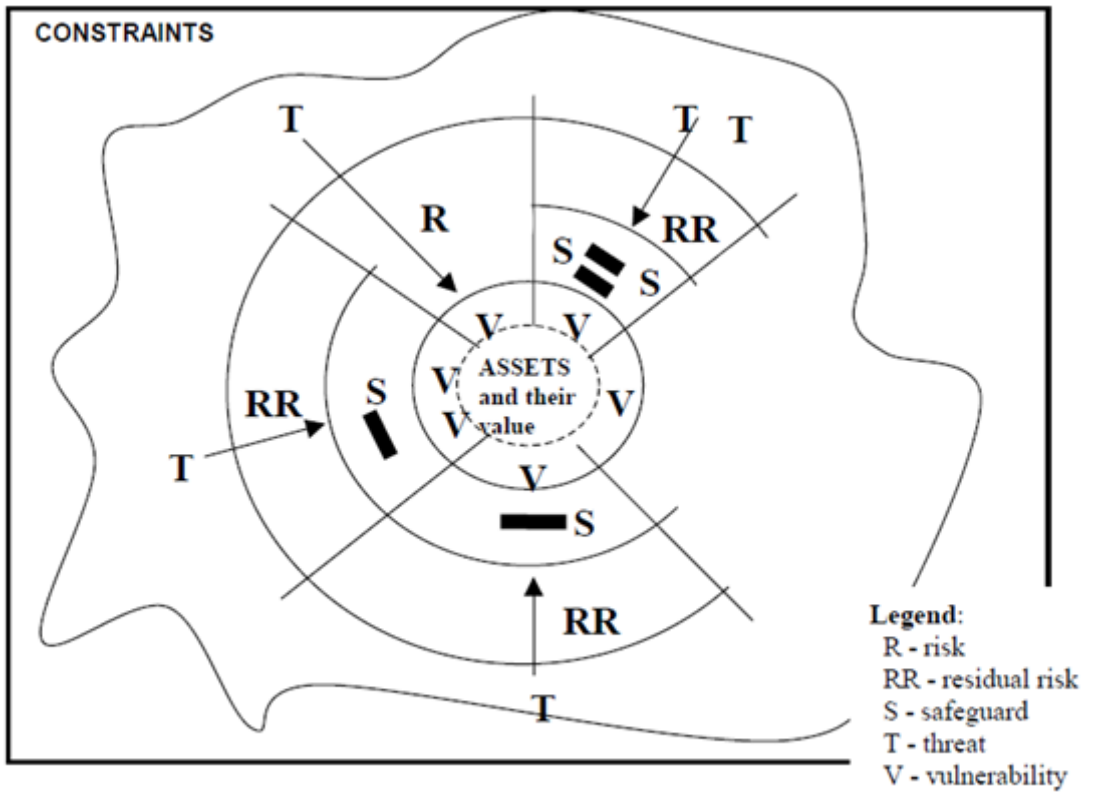

Figure 1 – Security element relationships

Dallo schema è chiaro che le vulnerabilità sono il centro dell'analisi e, quelle che non hanno ancora minacce in grado di sfruttarle, non necessariamente generano rischi (l'esempio fatto prima su Meltdown/Spectre e 0Day).

Quindi cosa fare se si ha una valutazione dei rischi che include minacce e vulnerabilità? Semplicemente capirne i contenuti e l'aderenza con la norma, decidere se vale comunque la pena di mantenerla come è oppure modificare il processo per adattarlo ai requisiti della ISO/IEC 27001.

È un errore parlare di minacce e vulnerabilità in una valutazione dei rischi per una ISO/IEC 27001? No, se assicura comunque la copertura delle informazioni e non diventa fuorviante per uno dei potenziali errori sopra descritti.

Cosa si fa se siamo incappati in uno di questi errori? Si riparte dalla ISO/IEC 27001 e poi si riconsidera il tutto per valutare se l'errore impatta o meno sulla sicurezza delle informazioni in modo significativo (esistono il livello di rischio accettabile e l'accettazione consapevole del rischio che possono venirci in aiuto in questi casi).

Cosa si rischia lasciando le cose come sono? Dal punto di vista formale, una non conformità come minimo, che può diventare maggiore/critica/bloccante in base al tipo di conseguenze sul Sistema di Gestione. Dal punto di vista sostanziale si avrebbe un Sistema concentrato su elementi errati e un dispendio di energie che non necessariamente assicura il grado di protezione atteso.

Un argomento così complesso non può essere risolto in queste poche righe ma da qualche parte dobbiamo pur iniziare a rimettere ordine. Partire da queste considerazioni può aiutare molte organizzazioni.