Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS

Ufficio federale della cibersicurezza UFCS
Analisi e prevenzione

2 luglio 2025

Valutazione tecnologica

Gestione della sicurezza delle informazioni e SGSI

1 Introduzione

Nella società dell'informazione, le informazioni rivestono un ruolo di spicco per le organizzazioni e le aziende: solitamente vengono cifrate come dati e poi salvate elettronicamente nonché elaborate e trasmesse. Vista la loro grande importanza, tali dati vanno protetti e resi sicuri nell'ottica di determinati obiettivi di protezione, come la confidenzialità, l'integrità (e/o l'autenticità) e la disponibilità. Questo tipo di protezione è un compito (gestionale) impegnativo – denominato ad esempio anche *gestione della sicurezza delle informazioni* – che viene opportunamente supportato da un *sistema di gestione della sicurezza delle informazioni (SGSI)*.

Nel quadro della presente valutazione tecnologica viene presentato l'SGSI, approfondendo di cosa si tratta esattamente, cosa è in grado di fare e come può supportare al meglio la persona e il gruppo di persone cui spetta garantire la sicurezza delle informazioni. È analizzata in particolare anche la questione relativa a cosa sono i (ciber-)rischi e come occorre affrontarli adeguatamente nel quadro di una gestione della sicurezza delle informazioni e di un sistema di gestione della sicurezza delle informazioni (SGSI). Va sottolineato che molte riflessioni si applicano anche ad altri sistemi gestionali e che un sistema gestionale va sempre osservato nel contesto di un modello (gestionale) in cui è possibile attuare una distinzione ad esempio tra livello politico, strategico, tattico e operativo. Qui di seguito non viene invece studiato ulteriormente l'inserimento di un SGSI (o di un altro sistema gestionale) in un simile modello.

2 Definizione dei termini

Per il termine «sistema di gestione della sicurezza delle informazioni (SGSI)» data la sua funzione di ampia valenza in letteratura esistono molte definizioni. Stando alla DIN EN ISO/IEC 27000[1] esso comprende ad esempio «la politica, le tecniche, le direttive nonché le risorse e le attività ivi correlate che vengono svolte e gestite da un'organizzazione per proteggere i propri valori informativi»: è dunque «un modello sistematico per l'introduzione, l'attuazione, lo svolgimento, la sorveglianza, la verifica, la gestione e il miglioramento della sicurezza delle informazioni di un'organizzazione, al fine di raggiungere i propri scopi aziendali». Una definizione un po' meno ampia e, quindi, più specifica figura in Wikipedia: un SGSI è «la

[1] Versione tedesca di ISO/IEC 27000:2016 Tecnologia dell'informazione – Tecniche di sicurezza – Gestione della sicurezza delle informazioni – Panoramica e vocabolario.

compilazione di procedure e regole all'interno di un'organizzazione che servono a definire durevolmente la sicurezza delle informazioni nonché a gestirla, controllarla, mantenerla intatta e migliorarla di continuo»[2]. Sulla scorta di quest'ultima definizione, l'Ufficio federale della cibersicurezza (UFCS) utilizza la seguente definizione orientata alla pratica come base per i suoi lavori in materia:

«Un SGSI è un sistema composto da procedure e regole che può essere impiegato in un'organizzazione o un'azienda per garantire la sicurezza delle informazioni: nella fattispecie è mirato a definire gli obiettivi concreti della sicurezza delle informazioni nonché a pianificarne, gestirne e garantirne il raggiungimento».

Nonostante secondo questa definizione un SGSI sia un sistema composto da procedure e regole e finalizzato a raggiungere gli obiettivi prestabiliti di sicurezza delle informazioni, tuttavia il concetto di sistema alla sua base rimane indefinito. Nel caso più semplice un SGSI può essere composto semplicemente da prescrizioni che sono formulate come procedure e regole oppure anche soltanto come l'elenco delle attività da eseguire regolarmente. Inoltre un SGSI può comprendere anche ausili e strumenti che supportano nel loro lavoro la persona o il gruppo di persone cui spetta garantire la gestione della sicurezza delle informazioni. Simili strumenti possono essere più o meno complessi. Purtroppo l'importanza di tali strumenti è spesso sopravvalutata oppure il concetto di un SGSI viene addirittura equiparato a quello di uno o più strumenti. Seguendo il detto[3] «a fool with a tool is still a fool» è anche possibile condividere l'opinione contraria, secondo cui il concetto di SGSI va definito indipendentemente dagli strumenti e non ha «a priori» nulla a che vedere con essi. Ciononostante dopo avere formulato per esteso un SGSI adeguato sorge il quesito con quale strumento o quali strumenti sia possibile attuare o supportare al meglio il SGSI. Tale quesito non può comunque né indirizzare né influenzare dal punto di vista del contenuto la specificazione di un SGSI. Ne consegue che è il SGSI a stabilire i requisiti che lo strumento deve rispettare, e non viceversa.

Oltre all'indipendenza di determinati strumenti, secondo l'UFCS vi è un secondo punto decisivo ai fini dell'impiego pratico di un SGSI: la comprensione dei rischi e il modo in cui vengono affrontati. Normalmente si prendono in esame i rischi derivanti da minacce esterne e interne (cioè i rischi dovuti alle minacce). In alternativa è però possibile prendere in considerazione anche i rischi che si limitano alle ripercussioni. Ad esempio in relazione al rischio di una perdita di dati è rilevante soprattutto la perdita di dati: in altre parole, per valutare il rischio derivante da una perdita di dati non riveste alcun ruolo determinante sapere se la perdita è stata causata da un errore umano, un malfunzionamento tecnico o un malware. Si tratta in ogni caso di un rischio che occorre assolutamente mitigare (ovvero ridurre), a prescindere dalla minaccia causale. Si può dunque provare a impostare una gestione della sicurezza delle informazioni unicamente in base a questo tipo di rischi (vale a dire i rischi dovuti alle ripercussioni). Ma prima vale la pena approfondire un po' di più il tema dell'approccio ai rischi.

3 Approccio ai rischi

Nel linguaggio comune per rischio si intende semplicemente una minaccia o un pericolo il cui superamento può risultare insidioso. Il concetto di rischio è infatti definito in maniera ampia e un determinato rischio può essere percepito, a livello soggettivo, in modi anche molti diversi.

---

[2] Gestione della sicurezza informatica - Wikipedia

[3] Benché l'origine di questo detto non sia del tutto chiara, di solito è attribuito all'informatico statunitense Grady Booch. Per rafforzarne ancora di più il messaggio centrale si potrebbe anche affermare: «A fool with a tool is a more foolish fool». In alternativa si può citare Abraham Maslow cui viene attribuito il seguente detto: «If all you have is a hammer, everything looks like a nail», ovvero un dato strumento non può di certo venire usato per risolvere qualsiasi problema.

Ciò vale persino per i rischi che sono quantificabili oggettivamente, come ad esempio il rischio che un aereo precipiti[4]. Ma per l'osservatore questi rischi sono invece astratti e vengono percepiti e valutati in maniera diversa da un individuo all'altro: vi sono persone che salgono quasi senza pensieri su un aereo mentre altre nelle medesime condizioni sviluppano una vera e propria aviofobia. Per entrambe le categorie il rischio, seppur identico, viene percepito e valutato su base individuale.

Nonostante la diversa percezione e valutazione dei rischi, a livello di cibersicurezza in generale e di gestione della sicurezza delle informazioni in particolare è opinione diffusa che sia possibile quantificare i rischi e prendere le decisioni di gestione della sicurezza delle informazioni sulla scorta di rischi quantificati. Si parla a tale proposito anche di approccio «basato sui rischi», intendendo di solito un approccio in cui per ogni minaccia, partendo da una quantità definita di minacce, è possibile calcolare un rischio singolo e un rischio complessivo quale somma di tutti i rischi singoli. Un rischio singolo viene stimato come il prodotto della probabilità di evento e dell'entità dei danni.

A lungo questa semplice formula dei rischi è prevalsa nel dibattito sulla sicurezza delle informazioni, anche in relazione al SGSI, e continua a farlo tuttora. Per motivare l'approccio basato sui rischi spesso si fa riferimento al settore assicurativo che da sempre quantifica i rischi, mettendo anche a punto un modello gestionale di successo. Ciò funziona per i rischi che conosciamo nella vita quotidiana e per i quali esistono documentazioni rilevanti, soprattutto a livello statistico, della probabilità di evento e della conseguente entità dei danni; un esempio è costituito dall'assicurazione furto o dall'assicurazione infortunio. Se invece per i rischi mancano simili documentazioni rilevanti a livello statistico, allora la situazione tecnica di assicurazione è più complessa. In tal caso a volte si lanciano comunque sul mercato soluzioni assicurative che in seguito vengono costantemente adattate in base ai valori delle esperienze fatte: simili offerte assicurative possono così svilupparsi nell'arco del tempo nonostante inizialmente non fosse chiaro come calcolare i rischi e come impostarle al meglio. È proprio quello che sta succedendo al momento anche nell'ambito della cibersicurezza: i clienti potenziali devono verificare nel singolo caso concreto le offerte assicurative proposte, che possono essere anche molto diverse per grado di copertura in caso di sinistro con danni e per portata delle prestazioni di sostegno. In nessun caso il semplice fatto che un'assicurazione sia proposta deve indurre a credere che tutti i rischi possibilmente correlati in tale ambito sono stati compresi, calcolati e quantificati. Laddove mancano dati affidabili si formulano ipotesi e la base di dati viene costituita nel corso del tempo.

Secondo l'UFCS un approccio orientato ai rischi è fondamentalmente corretto: tuttavia occorre ripensare e adattare il modo in cui i ciber-rischi (ovvero i rischi nel ciberspazio) vengono presi in considerazione e affrontati. Innanzitutto nel ciberspazio non esiste nessuna «quantità definita di minacce». E anche se esistesse, i singoli elementi che rappresentano una minaccia non sarebbero elementari e non potrebbero neppure venire elencati in maniera esaustiva. Di conseguenza non è possibile definire uno spazio sensato di probabilità[5]: a ben vedere la teoria delle probabilità non può quindi essere usata e il calcolo tramite le probabilità di evento non è definito e risulta del tutto arbitrario [1][6].

---

[4] Questo rischio può venire quantificato ad esempio dividendo il numero di disastri aerei per il numero di movimenti di volo (per unità di tempo e compagnia aerea).

[5] Dal punto di vista formale, uno spazio di probabilità è composto da uno spazio di evento e da una misura di probabilità che attribuisce a ogni evento una probabilità (cioè un numero reale tra 0 e 1), nel rispetto di tre assiomi di Kolmogorow.

[6] Eventualmente si potrebbe utilizzare la teoria delle probabilità definendo per ogni minaccia un rispettivo spazio di probabilità (composto da un unico elemento). Tuttavia in tal caso in un simile spazio di probabilità a ogni

Ma anche al di là di questa difficoltà formale è pressoché impossibile stimare le probabilità di minacce nel ciberspazio vista la mancanza di documentazioni statistiche e l'elevata dinamicità e complessità della materia. Ad esempio come stimare in maniera sensata la probabilità di una minaccia di fuga di dati? Infatti si potrebbe impiegare e motivare praticamente qualsiasi valore. Lo stesso vale anche per l'entità dei danni: anche in questo caso sarebbe possibile motivare quasi ogni importo, soprattutto se si prendono in considerazione gli eventuali danni successivi. Ad esempio un update errato in certe condizioni potrebbe causare un danno quasi impercettibile e trascurabile per entità mentre in altri casi (basti ricordare ad esempio il guasto «Crowdstrike» del 2024) si possono verificare danni miliardari, con stime finali dei danni che variano addirittura di svariati miliardi. A fronte di questa difficoltà nella stima della probabilità di evento e dell'entità dei danni non si può usare opportunamente la formula dei rischi sopracitata, a meno comunque di adattarla o completarla. Ma purtroppo fino ad oggi tale adattamento o ampliamento non è ancora avvenuto e, quindi, la formula dei rischi non è praticabile e in una certa qual misura appare persino illusoria.

Anziché adottare un approccio formale ai rischi, nella realtà in molti casi si preferisce affrontarli in maniera euristica [2, 3]. Come esempio si può prendere il modo di lavorare di un medico generico: per garantire la salute del paziente non tratta una quantità definita di malattie e non argomenta neppure avvalendosi di probabilità di evento e di entità dei danni. Cerca invece di constatare al meglio lo stato di salute del paziente servendosi di conoscenze di fondo e misurazioni specifiche per poi proporgli un trattamento farmacologico orientato agli obiettivi e basato su criteri euristici. Inoltre, indipendentemente dallo stato di salute del paziente, il medico gli suggerisce consigli fondamentali validi genericamente, come ad esempio una sana alimentazione e un'attività fisica regolare. Un simile approccio, che combina elementi di protezione di base con ulteriori specifiche orientate agli obiettivi, si presta bene anche per la cibersicurezza e/o nella gestione della sicurezza delle informazioni come pure nella costituzione e nell'esercizio di un SGSI.

4 Conclusioni e prospettive future

Un SGSI è destinato a supportare al meglio la persona o il gruppo di persone incaricate della gestione della sicurezza delle informazioni. Nonostante la funzione di supporto così preconizzata suggerisca che nel caso di un SGSI si tratti di uno strumento, questa caratteristica è solo secondaria. Infatti primariamente un SGSI è composto da procedure e regole che possono essere implementate nel quadro di uno strumento, anche se questo non è automatico. Nella gestione della sicurezza delle informazioni e nell'approccio ai ciber-rischi, oltre a focalizzarsi sulle procedure e sulle regole (anziché sugli strumenti) è opportuno anche abbandonare i calcoli dei rischi e sfruttare al loro posto gli approcci euristici. Come la salute in medicina anche la sicurezza nel ciberspazio è troppo complessa per potere essere ridotta a una semplice formula. Al contrario, i criteri euristici sono più adatti per essere all'altezza della complessità della cibersicurezza.

Sulla base di questi dati di fatto l'UFCS al momento sta elaborando un modo di procedere strutturato e un metodo volti a rafforzare la cibersicurezza e la resilienza. Il metodo viene reso accessibile pubblicamente e può essere usato da tutte le organizzazioni e le aziende indipendentemente dalle loro dimensioni e dal settore in cui operano: così saranno in grado di prepararsi in maniera orientata agli obiettivi e alle minacce rilevanti per esse stesse nonché di

minaccia dovrebbe poi essere attribuita anche la probabilità 1 (per rispettare gli assiomi di Kolmogorow) e questo mette in dubbio l'utilità dell'approccio nel suo complesso.

costituire e mettere in funzione un SGSI servendosi delle spiegazioni del presente documento. Naturalmente un simile SGSI potrà venire ampliato gradualmente e completato a molti livelli.

Bibliografia

[1] Andreas Grünert, James Bret Michael, Rolf Oppliger e Ruedi Rytz, Why Probabilities Cannot Be Used in Cyber Risk Management, *IEEE Computer*, vol. 57, n. 10, ottobre 2024, pagine 86 – 89

[2] Rolf Oppliger e Andreas Grünert, How to Manage Cyber Risks: Lessons Learnt from Medical Science, *IEEE Computer*, vol. 56, n. 1, gennaio 2023, pagine 117 – 119

[3] Rolf Oppliger e Andreas Grünert, How to Measure Cybersecurity and Why Heuristics Matter, *IEEE Computer*, vol. 57, n. 2, febbraio 2024, pagine 111 – 115