NIST Cybersecurity Framework: come valutare il profilo cyber di un'organizzazione

INDICE DEGLI ARGOMENTI

Cogliendo lo spunto del processo di aggiornamento del NIST Cybersecurity Framework (NIST CSF), è interessante vedere come valutare il profilo di sicurezza dall'azienda nel contrasto alle minacce di tipo cyber in modo semplice, efficace e cost-effective.

In Europa, il NIST Cybersecurity Framework ha costruito molto del suo successo per il legame privilegiato con la **Direttiva NIS** ("Network and Information Security Directive").

Benché apparentemente sia rivolto alle solo infrastrutture critiche, **il framework originale nasce come proposta implementativa su base volontaria estesa a tutti**, pur con le raccomandazioni del caso di valutare nella decisione di adozione del framework anche la propria rilevanza all'interno dell'ecosistema economico di appartenenza.

1 COS'È E A COSA SERVE IL NIST CYBERSECURITY FRAMEWORK

Il NIST CSF nasce nel febbraio 2013 a seguito dell'Executive Order 13636 ("Improving Critical Infrastructure Cybersecurity") del Presidente degli Stati Uniti d'America. L'obiettivo è quello di **creare un fronte comune di difesa contro le minacce di tipo cyber**, che sia il più ampio possibile.
Il punto di partenza è la consapevolezza delle proprie debolezze per comprendere la misura delle azioni di difesa necessarie considerando anche l'impatto sull'intera supply chain, ossia una valutazione dello stato di protezione attuato da ogni entità presente nell'ecosistema.

Il volano per coinvolgere quante più entità sia possibile, è stato quello di polarizzare l'attenzione sull'intera supply chain delle infrastrutture critiche, dando a tutte le entità, coinvolte o meno, una serie di vantaggi per la loro adesione su base volontaria.

I criteri costitutivi del CSF già fanno comprendere che il livello implementativo è alla portata di tutti. È semplice da comprendere ed implementare in quanto espresso in un linguaggio comune, non specialistico.

Non impone alcuna tecnologia o standard ma si adatta al contesto corrente. È un documento vivo, basato su standard internazionali ed aggiornato periodicamente con il contributo di esperti della materia.

L'attenzione ai costi è per principio importante e si trae beneficio anche da un sistema di condivisione delle informazioni su minacce, vulnerabilità e metodi di contrasto dei fenomeni avversi.

2

EVOLUZIONE DEL NIST CYBERSECURITY FRAMEWORK

A inizio 2024 sarà disponibile la nuova versione del CSF. Non modifica l'impostazione generale ma perfeziona l'insieme delle funzioni e delle categorie secondo una sequenza più razionale e pratica. La checklist del framework è una sequenza di risultati desiderati del sistema di protezione e la CSF 2.0 ne rivedrà l'ordine e la tassonomia.

Il totale delle funzioni crescerà di una unità, la Govern, in coerenza con il framework sulla privacy del NIST, ma l'insieme complessivo delle novità resta limitato in quanto si rivedono o si spostano elementi tra loro, piuttosto che introdurne di realmente nuovi.

Il vantaggio sarà un minore cambiamento, implementativo e concettuale, da apportare al processo di valutazione, inoltre la sequenza finale delle sottocategorie risulterà più intuitiva nel comprendere i risultati.

Senza entrare nel merito dei cambiamenti nella checklist, in quanto c'è l'attesa di un nuovo workshop in autunno per essere confermati o meno, è interessante vedere come cambia l'approccio per la valutazione del profilo di sicurezza.

Quest'ultima è stata senza dubbio la parte che ha visto più variazioni ed adattamenti implementativi nell'attuale versione del CSF. Non è assolutamente negativo, anzi è previsto dal framework stesso adottare il metodo ritenuto più conveniente e questa flessibilità è da considerarsi un valore aggiunto. Un metodo unico e condiviso porta dei vantaggi in

termini di confrontabilità dei risultati ma non sarebbe nello spirito del framework perché perderebbe in flessibilità.

La scelta della modalità di verifica periodica della completezza e dell'efficacia delle misure adottate è generalmente fatta a livello di Paese per avere una base nazionale uniforme di confronto delle valutazioni. Non è un vincolo critico. Si può continuare ad utilizzare il metodo scelto nella propria organizzazione e definire un algoritmo di conversione automatica nel proprio standard Paese per non perdere i benefici della flessibilità di scelta.

Nel corso degli ultimi anni sono comparsi dei metodi di valutazione del profilo di cyber security in aggiunta alla proposta NIST. Proveremo a vederne alcuni. Nel 2016, con la Direttiva NIS sulle infrastrutture critiche, il CSF, è risultato rilevante anche per il nostro Paese per tramite del Framework Nazionale sulla Cybersecurity.

Con una strada diversa, ma motivi similari dovuti alla crescente digitalizzazione e comparsa delle relative minacce, anche la Confederazione Svizzera ha adottato questo framework per definire lo standard minimo per le TIC (Tecnologie dell'Informazione e della Comunicazione).

3. VALUTAZIONE NIST, I LIVELLI DI IMPLEMENTAZIONE

Il NIST Cybersecurity Framework raccomanda una metrica, detta "implementation tiers", per valutare il rigore con cui un'organizzazione affronta la gestione del rischio di sicurezza informatica ed il grado di sofisticazione del relativo approccio gestionale.

Non è un metodo di immediata comprensione ma è completo nel dare una valutazione, sia rappresentativa del livello di implementazione del controllo di contenimento del rischio, che del livello di implementazione del processo di gestione del rischio.

In effetti, è una matrice e questo spaventa le prime volte i valutatori abituati ad una scelta puramente lineare. Si compone di una griglia rappresentativa del grado di implementazione con le colonne che rappresentano il controllo e le righe la gestione del rischio. La colonna di grado maggiore, ove tutte le sue righe sono soddisfatte, rappresenterà la misura cercata.

La proposta NIST CSF è una matrice di quattro colonne ("tiers") per tre righe. I tiers sulle colonne sono definiti dalle label:

"Partial": soluzioni ad hoc quando serve, senza troppe formalizzazioni;
"Risk Informed": soluzioni localizzate anche se con il supporto manageriale;
"Repeatable": soluzioni formalizzate e controllate sull'intero perimetro aziendale;
"Adaptive": soluzioni con condivisione esterna e processi decisionali basati sul rischio; mentre le righe rappresentano tre approcci progressivi di gestione del rischio, dalla semplice definizione del processo funzionale e ripetibile, al programma integrato con gli altri processi aziendali, fino alla completa condivisione con le parti interessate esterne (supply chain).

4 VALUTAZIONE DEL FRAMEWORK NAZIONALE

In Italia, il "Framework Nazionale per la Cybersecurity e la Data Protection" del febbraio 2019 adotta una variante del metodo originale NIST, eliminando la matrice ed aggiungendo nuovi elementi.

Degli Implementation Tiers rimangono solo le colonne ("Parziale", "Informato", "Ripetibile", "Adattivo"). In aggiunta ci sono i livelli di priorità per definire l'ordine del programma di implementazione delle misure per raggiungere i valori attesi del profilo target.

Inoltre, ci sono dei livelli di maturità da valutare per comprendere il grado raggiunto nell'implementazione del controllo. Allo stesso modo, possono essere utilizzati anche per definire lo stesso target da raggiungere.

Per finire, si fa ricorso a dei prototipi (template), personalizzati per ambito applicativo, definendo il livello di priorità, la classe di implementazione e la maturità per ciascuna subcategory selezionata, con eventuali sottolivelli di maturità per le categorie che necessitano maggior dettaglio.
In tal modo, chi deve valutare, riceve un aiuto per una miglior comprensione della situazione e fornisce una valutazione più pertinente al caso reale. Di contro, la necessaria omogeneità dei risultati nel confronto tra profili di organizzazioni diverse, fa perdere la contestualizzazione dovendo mantenere la maturità ad un livello rappresentativo comune.

5. VALUTAZIONE DELLO STANDARD MINIMO PER LE TIC

Anche la Svizzera ha adottato come riferimento per la sicurezza informatica il framework NIST, quale punto di partenza per proporre alle aziende ed alle pubbliche amministrazioni nazionali e cantonali un test di misura del livello di sicurezza infrastrutturale nelle varie realtà.

È nella forma di un questionario con le misure minime da adottare per la messa in sicurezza delle infrastrutture critiche e dei dati sensibili. La valutazione delle sottocategorie (mansioni) avviene tramite i tiers, semplificati dalla mancata esposizione dell'approccio adottato nella gestione del rischio, e descrivono un crescente grado di maturità secondo il seguente schema:

0 = mansione non attuata;
1 = mansione parzialmente attuata, non definita e approvata completamente;
2 = mansione parzialmente attuata, definita e approvata completamente;
3 = mansione attuata, completamente o in gran parte attuata, statica;
4 = mansione dinamica, attuata, verificata costantemente, migliorata.

Lo schema di valutazione ha quattro livelli di stima della maturità ed è lo stesso per ciascun contesto considerato. La semplicità e praticità d'uso predominano sulle altre caratteristiche.

6. VALUTAZIONE CON CAPABILITY MATURITY MODEL

Nel documento *"Metodologia per il cybersecurity assessment con il Framework Nazionale per la Cybersecurity e la Data Protection"* del settembre 2021 troviamo un'ulteriore metodo, ben noto in altri contesti, che include la valutazione tramite il classico modello di maturità della capacità di realizzazione.

Si segue uno schema metodologico a tre passi, a partire dalla definizione della contestualizzazione del framework alla realtà di interesse, definendo il profilo target. Quindi si individua la postura di sicurezza attuale, sia come copertura dei controlli che di maturità raggiunta. Infine, si valuta il gap tra il profilo attuale ed il target rilevato.

Il grado di copertura associato a un controllo è valutato semplicemente con una scala numerica compresa tra 0 (mancanza del controllo) e 1 (piena implementazione) e delle sfumature intermedie per ulteriore dettaglio. Il livello di maturità nell'implementazione del controllo è invece espresso attraverso la scala del Capability Maturity Model Integration (CMMI) che prevede cinque livelli.

Iniziale: soluzione generalmente ad-hoc;
Ripetibile: soluzione a livello di department;
Definito: processo ben definito;
Gestito: processo misurato sistematicamente;
Ottimizzato: processo basato sul principio del miglioramento continuo.

Il livello di maturità viene combinato con altri parametri per giungere a completare il profilo attuale.

La valutazione finale considera la differenza tra la definizione del profilo target giustificata dal livello di rischio ed il profilo attuale conseguenza dalla maturità rilevata. Dalla valutazione segue la determinazione delle risorse necessarie per migliorare fino ai valori prefissati.

7 CONCLUSIONI

La prossima versione del framework NIST CSF, in linea con i principi fondanti, avrà un approccio molto pragmatico come si può evincere dalle informazioni esposte nel loro sito. Poiché in pratica non esiste un unico metodo per misurare e valutare il CSF, il NIST non spingerà verso un unico approccio di valutazione nel CSF 2.0 al fine di mantenere la flessibilità nel modo in cui le organizzazioni possono implementare il framework.

Il CSF 2.0 includerà esempi di come le organizzazioni hanno utilizzato il CSF per valutare e comunicare le proprie capacità nella gestione della sicurezza informatica. Ci saranno esempi di come le organizzazioni potranno utilizzare il CSF, combinato con strategie di gestione del rischio e modelli di maturità, per comunicare i risultati di valutazione dell'efficacia della loro sicurezza informatica.

Considerando gli annunci sulle modalità di aggiornamento del NIST CSF ed i suoi principi fondanti, le aziende che non hanno ancora un processo di valutazione della sicurezza informatica, possono aderire al CSF 1.1 senza alcun timore di perdita di valore sul lavoro che verrà svolto.

Per chi ha già implementato il processo di valutazione, con gli esempi forniti dal NIST, può considerare eventuali semplificazioni o migliorie. In generale, le considerazioni per l'avvio di questo framework nel lontano 2013 sono tuttora completamente valide.

Solo dalla consapevolezza delle proprie debolezze si riesce a creare una protezione efficace.

NETWORK DIGITAL 360

Network Digital360 è il più grande network in Italia di testate e portali B2b dedicati ai temi della Trasformazione Digitale e dell'Innovazione Imprenditoriale, con oltre 50 fra portali, canali e newsletter.
Ha la missione di diffondere la cultura digitale e imprenditoriale nelle imprese e pubbliche amministrazioni italiane e di fornire a tutti i decisori che devono valutare investimenti tecnologici informazioni aggiornate e approfondite.
Il Network è parte integrante di Digital360HUB, il polo di Demand Generation di Digital360, che mette a disposizione delle tech company un'ampia gamma di servizi di comunicazione, storytelling, pr, content marketing, marketing automation, inbound marketing, lead generation, eventi e webinar.

VIA COPERNICO, 38
20125 - MILANO
TEL. 02 92852785
MAIL: MARKETING@DIGITAL4.BIZ