NIST Cybersecurity Framework 2.0

STORIA E CONTESTO DEL NIST CSF

Nel febbraio 2014, fu dunque rilasciata la prima edizione del “Framework for Improving Critical Infrastructure Cybersecurity”, destinato inizialmente ad aree come l’energia, i trasporti, le telecomunicazioni e la finanza.

Il merito principale del CSF è stato quello di strutturare la gestione dei rischi informatici intorno a un set di attività e risultati (“outcomes”) di alto livello, organizzati lungo cinque Funzioni: Identify, Protect, Detect, Respond e Recover.

Ogni Funzione è poi suddivisa in Categorie e Sotto-categorie, che dettagliano i risultati di sicurezza da perseguire. Al contempo, il CSF suggerisce di appoggiarsi a standard e best practice noti (come ISO 27001, COBIT, e le varie SP 800 di NIST stesso) per definire con precisione quali controlli adottare, lasciando però alle organizzazioni la libertà di scegliere in base alle proprie esigenze e allo scenario normativo di riferimento.

STORIA E CONTESTO DEL NIST CSF

Nel 2018, arrivò la versione 1.1, con alcune migliorie minori come l'aggiunta di guidance sul supply chain risk management e sullo scambio di informazioni relative alle minacce. Questa versione è rimasta in vigore fino ad oggi, con l'eccezione di piccole revisioni e aggiornamenti di contorno. Durante tutti questi anni, il NIST ha incoraggiato community e stakeholder a condividere casi d'uso e suggerimenti per rendere il Framework sempre più completo e flessibile, integrando aspetti emergenti come la privacy, l'intelligenza artificiale e, appunto, la blockchain.

La blockchain stessa, come tecnologia, non era al centro del dibattito sulla sicurezza informatica di inizio 2014. L'attenzione sul tema si è impennata tra il 2017 e il 2018 a causa del boom delle criptovalute e di progetti di innovazione nella finanza decentralizzata (DeFi).

Molti analisti e professionisti della sicurezza hanno cominciato a interrogarsi su come gestire i rischi tipici dei sistemi distribuiti basati su blockchain, incluse le vulnerabilità degli smart contract, la gestione delle chiavi crittografiche e i possibili attacchi ai protocolli di consenso (ad esempio attacchi del 51%). Vedremo in modo più approfondito come il CSF 1.1 possa fornire una struttura concettuale utile per affrontare queste sfide, pur non essendo pensato specificamente per il contesto blockchain.

STRUTTURA FONDAMENTALE DEL NIST CSF 1.1

1. **Identify (ID)**: riguarda l'analisi e la comprensione del contesto dell'organizzazione, la definizione delle risorse (asset) critiche, dei processi aziendali, dei ruoli e delle responsabilità, nonché l'individuazione delle minacce e delle vulnerabilità. L'obiettivo è costruire la consapevolezza del rischio in modo da poter poi adottare adeguate misure di protezione.

2. **Protect (PR)**: include tutte le misure di sicurezza (tecniche, organizzative e procedurali) volte a proteggere gli asset identificati. Si riferisce, ad esempio, a controlli di accesso, crittografia, segmentazione di rete, formazione del personale, implementazione di policy di sicurezza e procedure di backup.

3. **Detect (DE)**: si concentra sull'abilità di rilevare prontamente eventi anomali, attività sospette o veri e propri incidenti di sicurezza. Si parla di monitoraggio, logging, analisi dei log, sistemi di intrusion detection/prevention, analisi comportamentale e correlazione degli eventi di sicurezza.

4. **Respond (RS)**: affronta la capacità di reagire efficacemente a un incidente in corso, contenendo i danni, analizzando l'impatto e coordinando le comunicazioni interne ed esterne. Comprende anche la notifica degli stakeholder e l'avvio di procedure di emergenza.

5. **Recover (RC)**: è dedicata al ripristino delle normali operazioni dopo un incidente e al miglioramento continuo. Riguarda piani di disaster recovery, strategie di continuità operativa, riparazione delle vulnerabilità sfruttate e valutazione delle lezioni apprese.

STRUTTURA FONDAMENTALE DEL NIST CSF 1.1: Categorie e Subcategorie

Descrivono in maniera più granulare gli obiettivi di sicurezza.

Ad esempio, la Funzione Identify include la Categoria “Asset Management”, che a sua volta comprende Subcategorie come “ID.AM-1: Le risorse fisiche sono identificate e gestite in linea con la loro importanza per la strategia di sicurezza”. Oppure, la Funzione Protect include una Categoria dedicata alla protezione dei dati (Data Security), con Subcategorie che descrivono l’uso di metodi crittografici, la politica di accesso ai dati.

Ogni Subcategoria può essere poi associata a controlli specifici o standard di riferimento. Nelle tabelle del CSF 1.1 si trovano i cosiddetti “Informative References” verso fonti come ISO 27001:2013, COBIT 5, ISA 62443, NIST SP 800-53. L’idea è che il Framework dica “cosa” bisogna ottenere (outcome), mentre gli standard prescelti suggeriscano “come” implementarlo tecnicamente o proceduralmente.

STRUTTURA FONDAMENTALE DEL NIST CSF 1.1: Tiers e Profile

Un altro elemento chiave del CSF è la definizione di **Tiers** (livelli) per la gestione del rischio informatico, che vanno da Tier 1 (Partial) a Tier 4 (Adaptive).

I Tiers sono concepiti per caratterizzare la maturità con cui l'organizzazione affronta il rischio: ad esempio, a Tier 1 (Partial) prevale un approccio reattivo e privo di processi formalizzati, mentre a Tier 4 (Adaptive) l'azienda è altamente proattiva, integra la cybersecurity nella governance complessiva e si adatta costantemente ai cambiamenti del panorama di minaccia.

Inoltre, il CSF introduce il concetto di **Profile**, ossia una rappresentazione personalizzata del Framework in base al contesto specifico dell'organizzazione. Un "Current Profile" descrive la postura di sicurezza attuale, evidenziando quali Subcategorie sono soddisfatte e a che livello, mentre un "Target Profile" descrive l'assetto desiderato. L'analisi delle differenze tra Current e Target Profile aiuta a definire un piano di miglioramento continuo.

Tale impostazione modulare e personalizzabile rende il CSF 1.1 estremamente versatile. È ampiamente adottato in vari settori, sia pubblici che privati, perché non impone uno standard rigido di controlli, bensì offre un linguaggio e un quadro di riferimento entro cui ogni organizzazione può costruire (o migliorare) il proprio programma di cybersecurity.

INTEGRAZIONE DEL CSF 1.1 CON LA TECNOLOGIA BLOCKCHAIN

1. **Identify**: Un'organizzazione che utilizza la blockchain deve, innanzitutto, definire il perimetro del sistema distribuito, identificando i nodi partecipanti, i dati critici che vi transitano e i rischi specifici derivanti dall'uso di protocolli di consenso (proof of work, proof of stake, etc.). Anche la gestione delle chiavi crittografiche è cruciale.

2. **Protect**: Qui, l'uso della blockchain implica spesso di adottare misure di protezione non solo a livello di rete tradizionale (firewall, IDS, etc.), ma anche di definire policy robuste per la custodia di chiavi e credenziali. Se si tratta di smart contract, occorre un processo di revisione del codice per evitare vulnerabilità logiche. L'accesso ai nodi validatori, in blockchain permissioned, deve essere rigorosamente controllato.

3. **Detect**: Rilevare attività malevole in una blockchain pubblica può essere complesso, ma gli strumenti di analytics e i servizi di monitoraggio delle transazioni (alcuni basati su tecniche di intelligence) possono individuare comportamenti sospetti. Nelle blockchain permissioned, si può implementare un monitoraggio dei log dei nodi e identificare anomalie.

4. **Respond**: L'aspetto di risposta a incidenti in ambito blockchain è delicato: spesso, in reti pubbliche, non c'è una governance centralizzata in grado di "annullare" transazioni fraudolente. In reti private, si possono prevedere meccanismi di reazione più rapidi, ma serve comunque un piano di incident response condiviso tra i partecipanti.

5. **Recover**: Nel caso di un attacco riuscito o di una compromissione delle chiavi, bisogna definire come ripristinare la continuità operativa e l'integrità del ledger, tenendo conto che l'immutabilità della blockchain impedisce un rollback tradizionale. Occorre quindi progettare procedure di emergenza, backup e ridondanza dei nodi.

LIMITI E POSSIBILI AREE DI MIGLIORAMENTO DEL CSF 1.1

Nonostante il successo planetario, il NIST CSF 1.1 presenta alcune possibili criticità o limiti:

- **Governance**: molte organizzazioni hanno sottolineato la necessità di un maggiore approfondimento su ruoli e responsabilità a livello dirigenziale.
- **Supply Chain Risk Management**: era presente un cenno nel CSF 1.1, ma si auspicava un'integrazione più approfondita, poiché molte violazioni avvengono sfruttando i fornitori.
- **Mancanza di esempi operativi**: il Framework descrive outcome generali e lascia agli standard tecnici il "come", talvolta creando difficoltà alle PMI.
- **Nuove tecnologie**: la continua evoluzione (cloud, AI, IoT, blockchain) richiede aggiornamenti costanti.
- **Componente internazionale**: pur adottato su scala globale, il CSF è concepito in ambito statunitense e potrebbe giovare di maggiori riferimenti a normative di altre regioni.

Questi aspetti hanno spinto il NIST verso la revisione più ampia che sfocerà nel CSF 2.0, previsto nel 2024, dove spicca una nuova Funzione dedicata alla governance e un rafforzamento della parte su supply chain e risorse online aggiornabili.

TRANSIZIONE VERSO IL NIST CSF 2.0

- **Aggiunta della Funzione "Govern"**: per affrontare in modo esplicito governance del rischio, policy e ruoli a livello dirigenziale.
- **Più enfasi sulla Supply Chain**: Category dedicata e riferimenti più chiari a pratiche di C-SCRM.
- **Maggiore attenzione alle PMI**: Quick Start Guides e Implementation Examples mirati.
- **Integrazione con standard globali**: ulteriore mappatura a normative internazionali.
- **Approccio modulare con risorse online**: per mantenere il documento principale stabile e aggiornare dinamicamente le best practice.

È verosimile che ciò si riveli vantaggioso anche in progetti blockchain, dove questioni come la governance e la supply chain (reti consortili, fornitori di nodi) sono particolarmente rilevanti.

PROSPETTIVE SU GOVERNANCE E SUPPLY CHAIN NEL CSF 2.0

Con “Govern”, il CSF 2.0 punta ad allineare più esplicitamente la sicurezza informatica con l’Enterprise Risk Management (ERM) e con le strategie generali dell’organizzazione. Ad esempio, un’azienda con un Chief Information Security Officer (CISO) e un consiglio di amministrazione sensibile al cyber risk potrà trovare in questa Funzione una “casa” per tutti quei processi che riguardano la definizione di policy, il budget di sicurezza, l’individuazione dei KPI (Key Performance Indicators) e KRI (Key Risk Indicators) e la supervisione dell’implementazione delle altre Funzioni (Identify, Protect, Detect, Respond, Recover). In assenza di una chiara governance, spesso si assiste a una frammentazione degli sforzi di sicurezza o a una mancanza di supporto dall’alto che rende vano ogni tentativo di rafforzare la postura complessiva.

Inoltre, il CSF 2.0 promette di offrire più riferimenti concreti per la **supply chain**, attraverso una Category dedicata e diverse Subcategorie che spiegano come gestire i fornitori dal punto di vista del rischio informatico. Questo è particolarmente attuale se si pensa a quante violazioni importanti sono avvenute sfruttando debolezze nei fornitori (si pensi all’incidente SolarWinds o ad attacchi rivolti a piattaforme software di terze parti). Il concetto di Cyber Supply Chain Risk Management (C-SCRM) viene quindi rafforzato, e si prospetta che il Framework includa collegamenti più espliciti ai documenti NIST come la SP 800-161r1, che fornisce linee guida dettagliate sul tema.

INTEGRAZIONE DEL CSF 2.0 CON LE TECNOLOGIE EMERGENTI E RUOLO DELLA BLOCKCHAIN

Uno dei fattori che hanno spinto il NIST a rivedere il Framework è la crescente diffusione di tecnologie emergenti, tra cui intelligenza artificiale, Internet of Things e blockchain. Per ciascuna, le sfide di sicurezza possono essere molto diverse rispetto ai sistemi tradizionali. Nel caso della blockchain, alcuni scenari salienti includono:

- **Blockchain per la tracciabilità della filiera**: si integrano sensori IoT, piattaforme di data management e ledger distribuiti, generando rischi su più livelli.

- **Finanza decentralizzata (DeFi)**: protocolli che offrono servizi finanziari senza intermediari, ma che hanno registrato numerosi attacchi e vulnerabilità negli smart contract.

- **Blockchain per identità digitale**: la gestione di credenziali e identità su un registro immutabile pone sfide in termini di protezione e revoca delle chiavi.

Il NIST CSF 2.0, con maggiore enfasi su governance e supply chain, potrebbe fornire una base più solida anche per questi contesti. La governance chiara è cruciale quando più stakeholder condividono la blockchain, e la Funzione “Govern” potrà guidare la definizione di policy e processi decisionali.

LA SFIDA DEL DECENTRALIZED GOVERNANCE

In una blockchain pubblica e permissionless, come Ethereum o Bitcoin, non esiste un organo di governo formale che possa imporre un livello di sicurezza o coordinare la risposta a incidenti. I processi di emergenza (ad esempio un hard fork) si basano spesso su un consenso sociale. Il NIST CSF può fungere da quadro di riferimento, ma si scontra con l'assenza di un'autorità responsabile. Al contrario, nei contesti "permissioned" o "consortium blockchain", i partecipanti possono stipulare accordi, definire regole di onboarding dei nodi e pianificare risposte comuni agli incidenti. In questi casi, il CSF 2.0 si applica in modo più simile all'IT tradizionale, sebbene resti la necessità di gestire la natura distribuita del sistema.

TEMPI DI PUBBLICAZIONE E ADOZIONE DEL CSF 2.0

Il NIST ha indicato come orizzonte il 2024 per la versione finale del CSF 2.0. Durante il periodo di consultazione pubblica, gli stakeholder inviano feedback e suggerimenti. Una volta rilasciato il documento definitivo, è probabile un periodo di transizione dove le organizzazioni potranno gradualmente allinearsi. In parallelo, il NIST curerà il "CSF portfolio" di risorse online, comprendente:

- **Informative References** aggiornati (mapping tra Subcategorie e standard)
- **Implementation Examples**
- **Quick Start Guides**

Community Profiles (profili "collettivi" creati da settori o associazioni)