SINTESI SU CYBERSECURITY FRAMEWORK

FOR

ELECTRIC VEHICLE CHARGING INFRASTRUCTURE

Autore: Aldo Pedico –Cybersecurity & Privacy Consultant

Contatto: pedicoaldo@gmail.com

PREMESSA

*Nel 2023, negli Stati Uniti risultano oltre 48.000 stazioni di ricarica pubbliche; entro il 2030 è previsto un impegno, da parte dell'*INFRASTRUCTURE INVESTMENT AND JOBS ACT, *per aumentare le stazioni a 500.000.*

*Le dimensioni del mercato delle infrastrutture di ricarica (*ELECTRIC VEHICLES - EV*) negli Stati Uniti sono state valutate a $3,15 miliardi nel 2022 e dovrebbero crescere fino a $24 miliardi entro il 2030. [Grandview]*

Attualmente, ci sono circa 2 milioni di veicoli elettrici in funzione ed il numero dovrebbe essere di 24,6 milioni entro il 2030 [EEI-2022].

In seguito: i) al valore attuale; ii) alla crescita prevista; iii) al potenziale di attacchi informatici; iv) alla criticità dei settori dei trasporti e dell'energia il DEPARTMENT OF ENERGY (DOE) *in collaborazione con l'*ELECTRIC POWER RESEARCH INSTITUTE (EPRI) *ha studiato l'ecosistema* ELECTRIC VEHICLE/EXTREME FAST CHARGING (ECOSISTEMA EV/XFC).

Riconoscendo la necessità per le parti interessate di valutare la loro posizione di sicurezza informatica come parte della gestione del rischio, DOE *ha commissionato a* NIST *l'applicazione del* CSF (CYBER SECURITY FRAMEWORK) *all'ecosistema* EV/XFC.

Ciò premesso, ritengo che l'argomento sia estremamente attuale anche se, al giorno d'oggi, non è percepito nella realtà dei fatti come un problema. Tuttavia, è bene per gli addetti ai lavori prendere in considerazione gli sviluppi futuri, i quali saranno la causa dell'ampliamento della superficie delle minacce, iniziando a pensare già da adesso ad adottare le contromisure necessarie a garantire l'affidabilità dei sistemi.

Il documento originale dal quale ho tratto questa mia sintesi è il "NIST IR 8473 - CYBERSECURITY FRAMEWORK PROFILE FOR ELECTRIC VEHICLE EXTREME FAST CHARGING INFRASTRUCTURE" liberamente fruibile da Internet.

INDICE DEGLI ARGOMENTI

Titolo **Pag.**

INTRODUZIONE

CYBERSECURITY FRAMEWORK PROFILE *sviluppato per l'ecosistema* ELECTRIC VEHICLE EXTREME FAST CHARGING (EV/XFC) *e le funzioni sussidiarie supportano ciascuno i quattro domini:*

(i) *Veicoli Elettrici* (EV);

(ii) *Ricarica Estremamente Rapida* (XFC);

(iii) XFC *Cloud o operazioni di terze parti;*

(iv) *Utility e Reti di Edifici.*

I riferimenti informativi elencati in "Ecosistema" *possono fornire informazioni aggiuntive o pratiche per qualsiasi membro dell'ecosistema, mentre i riferimenti elencati nei domini specifici* (EV, XFC/EVSE, *Cloud/Terze parti, Utility/Sistemi di gestione degli edifici) possono fornire informazioni o pratiche per quel dominio.*

Il profilo del quadro di sicurezza informatica per l'infrastruttura di XFC (*di seguito denominato profilo di sicurezza informatica* EV/XFC) *è un profilo a livello di settore; questo profilo fornisce un profilo di base che gli interessati possono utilizzare per svilupparne altri specifici per la loro organizzazione allo scopo di valutare la loro posizione di sicurezza informatica come parte del loro processo di gestione del rischio.*

Il profilo ha lo scopo di integrare ma non sostituire un programma di gestione del rischio esistente o gli attuali standard, regolamenti e linee guida del settore della sicurezza informatica attualmente in uso nel settore EV/XFC.

EV/XFC

- "Che cosa è" *e* "a che cosa serve" *il* PROFILO *di sicurezza informatica* EV/XFC:

  1) *è un'applicazione delle* CATEGORIE *e* SOTTOCATEGORIE *del framework nel contesto dell'ecosistema di sicurezza informatica* EV/XFC *fornito dal* DOE *e dall'*EPRI.
  2) *fornisce alle parti rilevanti per l'ecosistema un mezzo per valutare e comunicare la loro posizione di sicurezza informatica in modo coerente con il* Cybersecurity Framework.
  3) *offre agli utenti un approccio basato sul rischio a livello di settore per la gestione delle attività di sicurezza informatica e facilita la collaborazione incrociata tra le varie parti interessate del settore, i fornitori e gli utenti finali.*

- *L'utilizzo del* PROFILO *aiuterà le organizzazioni a:*

  1) IDENTIFICARE *le risorse e le interfacce chiave in ciascuno dei domini dell'ecosistema;*
  2) AFFRONTARE *i rischi di sicurezza informatica nella gestione e nell'utilizzo dei servizi* EV/XFC;
  3) IDENTIFICARE *le minacce, le vulnerabilità e i rischi associati ai servizi, alle apparecchiature e ai dati* EV/XFC;
  4) APPLICARE *i meccanismi di protezione per ridurre il rischio a livelli gestibili;*
  5) RILEVARE *le interruzioni e le manipolazioni dei servizi* EV/XFC;
  6) RISPONDERE *e* RIPRISTINARE *le anomalie del servizio* EV/XFC *in modo tempestivo, efficace e resiliente.*

➢ *L'ecosistema EV/XFC si basa su più domini connessi.*

Il PROFILO *si rivolge ai* quattro *domini principali dell'ecosistema* EV/XFC.

1. EV
   - ✓ *I veicoli elettrici sono disponibili in una varietà di forme e dimensioni: motociclette, automobili, velivoli* EVTOL (ELECTRIC VEHICLE TAKE-OFF AND LANDING) *come droni o aerei e veicoli commerciali (ad esempio, rimorchi per trattori, veicoli da costruzione, autobus).*
   - ✓ *I veicoli elettrici si basano su più sistemi di rete per comunicare internamente e con entità esterne.*
   - ✓ *Internamente sono presenti sistemi di controllo per batterie, motori, ricarica e il veicolo stesso che opera attraverso una* CONTROL AREA NETWORK (CAN) *interna.*
   - ✓ *Il caricabatterie e il veicolo comunicano attraverso un connettore fisico.*
   - ✓ *Il veicolo comunica con organizzazioni cloud di terze parti del fornitore tramite Bluetooth, Wi-Fi o cellulare.*

2. XFC/EVSE
   - ✓ *Le apparecchiature di alimentazione dei veicoli elettrici (*ELECTRIC VEHICLE SUPPLY EQUIPMENT - EVSE*) sono sistemi che forniscono energia elettrica al veicolo per ricaricare le batterie del veicolo.*
     I sistemi EVSE *includono conduttori elettrici, apparecchiature correlate come i sistemi di accumulo di energia della batteria (*BATTERY ENERGY STORAGE SYSTEM - BESS*), software e protocolli di comunicazione che forniscono energia in modo efficiente e sicuro al veicolo.*
   - ✓ EXTREME FAST CHARGING (XFC) *è un tipo di* EVSE *in grado di ricaricare i veicoli in pochi minuti anziché ore.*
   - ✓ XFC/EVSE *e le relative apparecchiature devono connettersi e comunicare con fornitori di cloud e di terze parti per procurare informazioni sulla posizione* EVSE, *fatturazione e altri servizi, oltre a connettersi al veicolo.*

3. CLOUD/THIRD-PARTY ORGANIZATIONS

- ✓ *L'ecosistema* EV/XFC *è costituito da domini di proprietà ed essi sono gestiti in modo indipendente; la maggior parte delle stazioni di ricarica sono gestite da una rete di ricarica con modelli di business che fondono insieme le vendite di stazioni di ricarica di stazioni elettriche, elettricità e veicoli.*
- ✓ *Le terze parti sono individui o entità che facilitano le transazioni ma non sono una delle parti primarie all'interno dello scambio.*
- ✓ *L'ecosistema* EV/XFC *utilizza in genere fornitori di servizi cloud per queste transazioni perché sono adatti per scambi di dati sensibili che coinvolgono informazioni finanziarie, informazioni di identificazione personale e altri dati potenzialmente sensibili.*

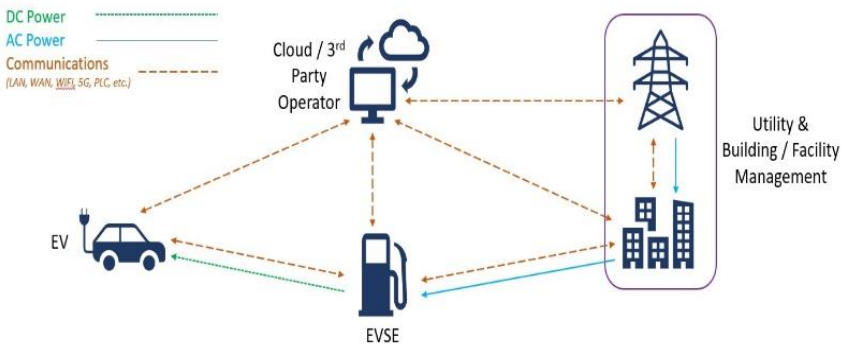
4. UTILITIES/SISTEMI DI COSTRUZIONE

- ✓ *Le utility forniscono l'energia necessaria per alimentare l'ecosistema* EV/XFC.
- ✓ *I sistemi di gestione degli edifici e delle strutture possono essere presenti in installazioni in cui è richiesta la gestione dell'energia, come* EVSE *installato nei centri commerciali, nonché dove possono essere presenti risorse energetiche distribuite (*DISTRIBUTED ENERGY RESOURCES - DER*) o dove è richiesto il controllo di sicurezza fisica.*
- ✓ *Sia i servizi pubblici sia i sistemi di gestione degli edifici/strutture includono apparecchiature per monitorare l'utilizzo dell'energia, comunicare con dispositivi collegati in rete e sistemi di supervisione e aiutare a controllare le richieste energetiche in loco.*

La gestione dei rischi di sicurezza informatica è importante per i processi IT *e* OT, *ma ci sono notevoli differenze operative tra i due che possono influire sull'implementazione delle tecniche di gestione del rischio per* IT *vs* OT. *Nonostante queste differenze, le interdipendenze tra* IT *e* OT *sono in aumento, il che porta a una crescente dipendenza* dell'OT *dai processi* IT *e possibilmente a vulnerabilità e rischi ereditati tra le due tecnologie.*

EV/XFC ECOSYSTEM DOMAINS AND PROFILE SCOPE

I concetti fondamentali utilizzati per definire l'ambito del profilo di sicurezza informatica EV/XFC *sono stati derivati da precedenti ricerche e documentazione sviluppate dall'*ELECTRIC POWER RESEARCH INSTITUTE *[EPRI-2023] come illustrato nella figura accanto.*



La generazione di energia e le comunicazioni all'interno dell'utility non rientrano nell'ambito del profilo di sicurezza informatica EV/XFC.

EV/XFC CYBERSECURITY MISSION OBJECTIVES (MO)

Gli EV/XFC CYBERSECURITY MISSION OBJECTIVES (MO) *forniscono il contesto per un'organizzazione necessario a gestire il proprio rischio di sicurezza informatica in relazione alle sue specifiche esigenze di missione. I seguenti obiettivi possono servire come base per una organizzazione al fine di definire i propri* MO *di sicurezza informatica.*

MO-1: DELIVER RELIABLE PERFORMANCE THROUGH SECURE COMMUNICATIONS

La comunicazione attraverso l'infrastruttura XFC *è fondamentale per le prestazioni nell'ecosistema* EV/XFC *e per il successo del settore* EV. *A causa di questa dipendenza in* "tandem", *le comunicazioni dovrebbero essere affidabili e sicure per soddisfare le esigenze di missione dell'ecosistema, pertanto è necessaria una maggiore attenzione alla sicurezza delle comunicazioni.*

La logica di questo obiettivo della missione include:

1) EV
   - ✓ *La comunicazione tra il veicolo elettrico (sistema di gestione della batteria) e la stazione di ricarica necessaria a facilitare il processo di ricarica della batteria* EV.
   - ✓ EV *si connette ad applicazioni cloud/terze parti per gestire le transazioni e raccogliere dati.*
   - ✓ *I sistemi utente* EV *(ad es. infotainment) possono anche comunicare con altri sistemi del veicolo, come il controller di carica e i sistemi di gestione della batteria.*
   - ✓ *L'interfaccia tra queste applicazioni presenta una potenziale superficie di attacco per gli attori malintenzionati.*

2) XFC/EVSE
   - ✓ *La stazione di ricarica richiede una comunicazione sicura con il cloud per facilitare le transazioni finanziarie, fornire l'autorizzazione per la ricarica, raccogliere i registri di manutenzione e ricevere aggiornamenti.*
   - ✓ *La stazione di ricarica attinge energia misurata.*

3) CLOUD/TERZE PARTI

- ✓ *I provider di servizi cloud richiedono connessioni sicure affidabili all'*EV*, alla stazione di ricarica e all'utility per facilitare il processo di ricarica.*
- ✓ *Le comunicazioni sicure e affidabili consentono la convalida delle transazioni finanziarie, proteggono le informazioni personali e consentono di trasmettere aggiornamenti e registri di manutenzione in modo rapido ed economico.*

4) SISTEMI DI GESTIONE DELLE UTENZE/EDIFICI

- ✓ *Le utenze forniscono energia alla stazione di ricarica.*
- ✓ *Coordinamento tra i caricabatterie* XFC *e le utility necessario per varie applicazioni smart grid come la riduzione dei picchi/spostamento del carico o la previsione.*
- ✓ *Laddove esiste la comunicazione, questa deve essere affidabile e sicura.*

MO-2: : MAINTAIN RESILIENCE OF THE XFC INFRASTRUCTURE

Tutti gli utenti dell'ecosistema EV/XFC *dovrebbero avere un accesso affidabile ai servizi.*

Una perdita di sicurezza informatica può influire sulla sicurezza fisica, pertanto le organizzazioni devono implementare misure di salvaguardia per garantire la resilienza dell'ecosistema EV/XFC.

La logica di questo obiettivo della missione include:

1) EV

- ✓ *I proprietari di veicoli elettrici vogliono la certezza che il loro veicolo sia protetto prima di essere disposti a partecipare all'ecosistema di ricarica.*
- ✓ *Le batterie sono una spesa significativa e un ecosistema* XFC *compromesso potrebbe potenzialmente causare danni fisici alla batteria, componenti* EV *e altre apparecchiature nelle vicinanze.*
- ✓ *Le misure di sicurezza implementate faciliteranno incoraggeranno l'uso delle stazioni di ricarica.*

2) XFC/EVSE

- ✓ *A causa della posizione unica delle stazioni di ricarica nell'ecosistema, della sua dispersione geografica e della sua generale mancanza di sicurezza fisica le stazioni di ricarica sono diventate un obiettivo attraente per i malintenzionati.*
- ✓ *Le infrastrutture EVSE dovrebbero essere protette per prevenire attacchi come ransomware o danni all'infrastruttura di ricarica stessa.*

3) CLOUD/TERZE PARTI

- ✓ *L'ambiente cloud/terze parti facilita la connettività tra i domini dell'infrastruttura.*

4) SISTEMI DI GESTIONE DELLE UTENZE/EDIFICI.

- ✓ *Le utility dovrebbero disporre di sistemi di protezione per prevenire la manipolazione dei componenti mantenendo operazioni sicure.*

MO-3: BUILD AND MAINTAIN TRUSTWORTHY RELATIONSHIPS WITH PARTNERS AND CUSTOMERS

La sicurezza informatica EV/XFC *richiede la raccolta e l'utilizzo dei dati di partner e clienti provenienti da molte fonti. Le organizzazioni considerino e mitighino i rischi durante l'intero ciclo di vita delle informazioni. La protezione della riservatezza delle informazioni (ad esempio, le informazioni sullo stato del sistema) garantisce la fiducia nell'organizzazione e stabilisce la fiducia tra i partner e con i clienti.*
Anche le informazioni personali dovrebbero essere protette (ad esempio, informazioni sulla carta di credito, modelli di utilizzo XFC *individuali) per garantire che le informazioni dell'utente non siano correlate per un uso inappropriato, con conseguente perdita di fiducia da parte degli utenti.*

La logica di questo obiettivo della missione include:

1) EV
   - ✓ *I proprietari di veicoli elettrici confidano che le stazioni di ricarica siano disponibili ed utilizzabili, non si danneggino durante la ricarica e proteggano le loro informazioni durante le transazioni.*

2) XFC/EVSE
   - ✓ *Gli* EVSE *sono la rappresentazione più visibile dell'ecosistema* EV/XFC *e un incidente informatico può avere un ampio impatto lasciando il pubblico incerto sulla sicurezza e l'affidabilità dei veicoli elettrici, potenzialmente influenzando le vendite future.*

3) CLOUD/TERZE PARTI
   - ✓ *I fornitori cloud e terze parti acquisiscono e mantengono informazioni finanziarie per le transazioni nell'ecosistema* EV/XFC.
   - ✓ *Il rilascio involontario di queste informazioni può comportare una perdita di fiducia da parte di tutte le parti rilevanti dell'ecosistema e comportare costi elevati per i fornitori cloud/terze parti a causa di sanzioni, cause civili o risarcimenti ai clienti.*

4) SISTEMI DI GESTIONE DELLE UTENZE/EDIFICI
   - ✓ *Le interruzioni nell'alimentazione elettrica possono: 1) lasciare i proprietari di veicoli elettrici bloccati; 2) altri nell'ecosistema* EV/XFC *incapaci di svolgere le loro funzioni aziendali.*

MO-4: MAINTAIN CONTINUITY OF OPERATIONS

L'ecosistema EV/XFC *deve sostenere le operazioni e garantire che la missione dell'organizzazione continui di fronte alle avversità.*

Le organizzazioni devono monitorare le deviazioni per identificare potenziali eventi di sicurezza informatica e rilevare e rispondere a comportamenti anomali.

Anche i processi di gestione del rischio della catena di approvvigionamento informatica dovrebbero essere identificati e concordati dalle parti interessate dell'organizzazione.

Inoltre, le organizzazioni tengono conto delle interruzioni attraverso la pianificazione della continuità aziendale/emergenza e l'implementazione di piani di risposta e ripristino.

La logica di questo obiettivo della missione include:

1) EV
   - ✓ *Capire quando un veicolo elettrico è compromesso o agisce al di fuori del suo normale funzionamento di base è fondamentale per un suo funzionamento sicuro e affidabile.*

2) XCF/EVSE
   - ✓ *Per rilevare comportamenti anomali, è necessario comprendere il profilo del ciclo di ricarica e il consumo energetico delle stazioni per identificare le deviazioni dalle normali operazioni che potrebbero indicare comportamenti dannosi.*
   - ✓ *I problemi della catena di fornitura (ad esempio, qualità, integrità, disponibilità) influiscono sull'affidabilità di* EVSE.

3) CLOUD/TERZE PARTI
   - ✓ *Le entità cloud/terze parti devono essere in grado di identificare comportamenti dannosi che si discostano dalle linee di base della sicurezza informatica (ad esempio, connessioni e/o trasmissioni sconosciute o nuove da fonti diverse dal fornitore di servizi o autorizzate dal fornitore di servizi).*

4) SISTEMI DI GESTIONE DELLE UTENZE/EDIFICI
   - ✓ *Le utility in genere dispongono di programmi per rilevare attività anomale da sistemi esterni che potrebbero influire sulle operazioni.*

OVERVIEW OF THE CYBERSECURITY FRAMEWORK (CSF)

CSF *aiuta le organizzazioni a gestire e ridurre meglio i rischi di sicurezza informatica in modo da rispondere alle esigenze, ai rischi, alle minacce e/o alla sofisticazione informatica specifici del settore (indipendentemente dalle sue dimensioni).*

Il Framework:

1) FORNISCE *un approccio all'analisi del rischio di sicurezza informatica, consentendo alle aziende di comprendere le loro sfide di sicurezza informatica e selezionando strategie di mitigazione appropriate.*
2) ENFATIZZA *il processo di gestione del rischio per la sicurezza informatica affermando che "il Framework si concentra sull'utilizzo di driver di business per guidare le attività di sicurezza informatica e considerare i rischi di sicurezza informatica come parte del processo di gestione del rischio dell'organizzazione" [NIST-CSF].*
3) PRESENTA *standard, linee guida e pratiche del settore in modo da consentire alle attività e ai risultati della sicurezza informatica di essere comunicati chiaramente a tutti i livelli di un'organizzazione, dai dirigenti agli individui con ruoli lavorativi operativi.*
4) FORNISCE *una tassonomia e un meccanismo comuni per le organizzazioni, basandosi su standard, linee guida e pratiche, allo scopo di:*
   - descrivere *la loro attuale posizione di sicurezza informatica;*
   - descrivere *il loro stato target per la sicurezza informatica;*
   - identificare *e* dare *priorità alle opportunità di miglioramento nel contesto di un processo continuo e ripetibile;*
   - valutare *lo stato di avanzamento verso lo stato di destinazione;*
   - comunicare *tra le parti interessate interne ed esterne in merito al rischio di sicurezza informatica.*

LE TRE COMPONENTI PRINCIPALI DEL FRAMEWORK

1. CORE: *è un catalogo di attività di sicurezza informatica e dei loro risultati scritti in un linguaggio comune.*
2. PROFILI: *è un allineamento dei requisiti organizzativi, degli obiettivi, della propensione al rischio e delle risorse rispetto ai risultati desiderati del* FRAMEWORK CORE.
3. LIVELLI DI IMPLEMENTAZIONE: *guidano le organizzazioni a considerare il livello appropriato di rigore per il loro programma di sicurezza informatica e possono essere utilizzati come strumento di comunicazione per discutere la propensione al rischio, la priorità della missione e il budget; ulteriori discussioni sui livelli di implementazione non sono incluse in questo profilo.*

THE CORE

CORE *è costituito da cinque funzioni [NIST-CSF].*

1. IDENTIFY
   - ✓ *Le attività della funzione* IDENTIFY *sono la base per un uso efficace del Framework.*
   - ✓ *Comprendere il contesto aziendale, le risorse che supportano le funzioni critiche e i relativi rischi di sicurezza informatica consente a un'organizzazione di concentrarsi e dare priorità ai propri sforzi, in linea con la propria strategia di gestione del rischio e le esigenze aziendali.*
2. PROTECT
   - ✓ *Supporta la capacità di limitare o contenere l'impatto di un potenziale evento di sicurezza informatica.*
3. DETECT
   - ✓ *Consente il rilevamento tempestivo degli eventi di sicurezza informatica.*
4. RESPOND
   - ✓ *Supporta la capacità di contenere l'impatto di un potenziale evento di sicurezza informatica.*
5. RECOVER
   - ✓ *Supporta il ripristino tempestivo delle normali operazioni per ridurre l'impatto di un evento di sicurezza informatica.*

Il Framework identifica inoltre le CATEGORIE *e le* SOTTOCATEGORIE *chiave sottostanti per ciascuna funzione e le abbina con riferimenti informativi di esempio come standard, linee guida e pratiche esistenti per ciascuna sottocategoria.*

La tabella 1 illustra l'allineamento delle categorie alle funzioni.

TABLE 1. FUNCTION AND CATEGORY UNIQUE IDENTIFIERS

FUNCTION	FUNCTION UNIQUE IDENTIFIER	CATEGORY	CATEGORY UNIQUE IDENTIFIER
IDENTIFY	ID	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
		Supply Chain Risk Management	ID.SC
PROTECT	PR	*Access Control*	PR.AC
		Awareness and Training	PR.AT
		Data Security	PR.DS
		Information Protection Processes and Procedures	PR.IP
		Maintenance	PR.MA
		Protective Technology	PR.PT
DETECT	DE	*Anomalies and Events*	DE.AE
		Security Continuous Monitoring	DE.CM
		Detection Processes	DE.DP
RESPOND	RS	*Response Planning*	RS.RP
		Communications	RS.CO
		Analysis	RS.AN
		Mitigation	RS.MI
		Improvements0	RS.IM
RECOVER	RC	*Recovery Planning*	RC.RP
		Improvements	RC.IM
		Communications	RC.CO

Le CATEGORIE *del Framework si suddividono in* SOTTOCATEGORIE, *queste sono attività di cibersicurezza più dettagliate e risultati specifici di attività tecniche e/o gestionali.*

I componenti finali del CORE *sono riferimenti informativi aventi lo scopo di mappare le* SOTTOCATEGORIE *e fornire al lettore standard, linee guida e pratiche esistenti che possano aiutare un'organizzazione a raggiungere il risultato desiderato per ciascuna* SOTTOCATEGORIA.

Lo sviluppo del profilo applica il Cybersecurity Framework concentrandosi sulle aree di sicurezza informatica di particolare interesse per un settore, un'organizzazione o un'area funzionale identificata attraverso i suoi processi di gestione del rischio.

I profili sono utilizzati per identificare le opportunità per migliorare la posizione di sicurezza informatica di un'organizzazione creando e confrontando un profilo "corrente" *(lo stato* "così com'è"*) con un profilo* "target" *(lo stato* "to be"*).*

All'interno di un'organizzazione, i profili offrono un modo coerente per discutere gli obiettivi di sicurezza informatica in tutti i ruoli dell'organizzazione o dell'agenzia, dalla leadership senior agli implementatori tecnici, utilizzando una terminologia comune.

XFC BASELINE PROFILE

Il profilo di base è costituito da tabelle per ogni categoria che riassumono il modo in cui ogni sottocategoria associata si applica in generale all'ecosistema EV/XFC *con riferimenti informativi per ulteriori indicazioni.*

Le tabelle forniscono considerazioni specifiche del dominio, a seconda dei casi.

In base alla progettazione, il Cybersecurity Framework è intrinsecamente flessibile per adattarsi agli ambienti e alle esigenze uniche delle diverse organizzazioni ed il suo utilizzo permetterà di comprendere le deviazioni tra la propria azienda e le ipotesi fatte in questo profilo possono influire sull'applicabilità delle sottocategorie.

Pertanto, si consiglia alle parti interessate di rivedere tutte le sottocategorie nel contesto della loro organizzazione.

Attenzione: per motivi pratici non ho riportato in questa sintesi l'elenco dettagliato delle Categorie/Sottocategorie ed i relativi controlli, pertanto chi fosse interessato può consultare il Capitolo "5. XFC BASELINE PROFILE" del manuale "NIST IR 8473".