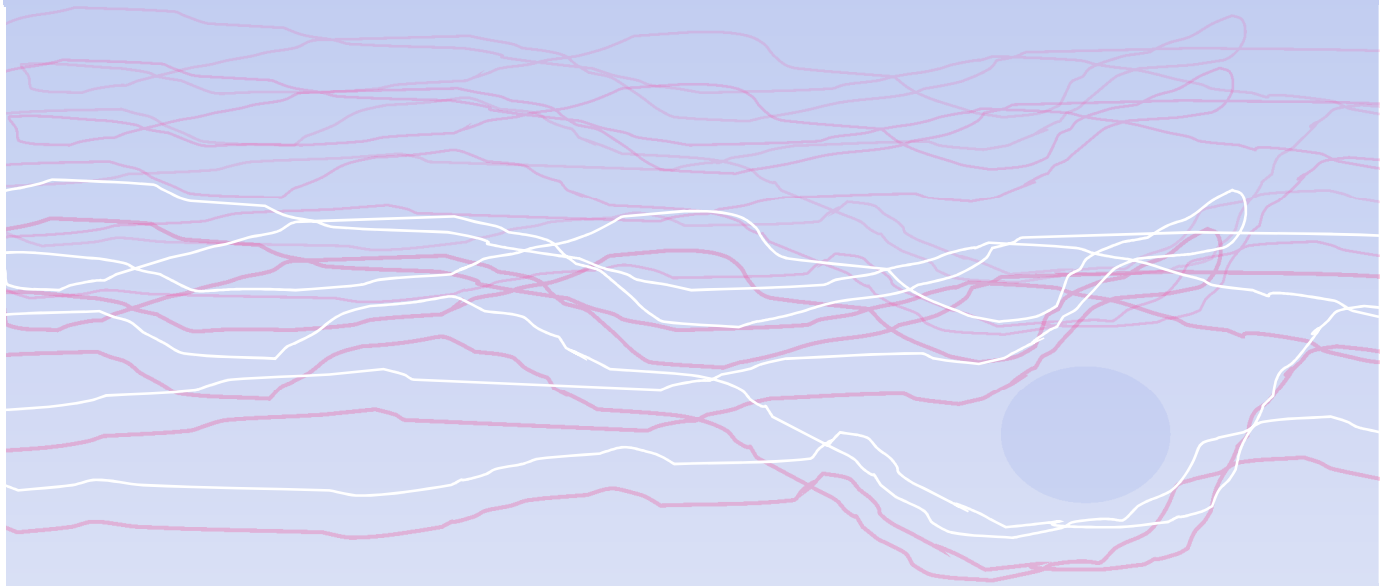
Principi, Linee Guida e Good Practices per la gestione della Cyber Security, Resilienza e Business Continuity degli Operatori Elettrici



Realizzato dall'Osservatorio Nazionale per la Cyber Security, Resilienza e Business Continuity delle Reti Elettriche

L'Osservatorio Nazionale per la Cyber Security, Resilienza e Business Continuity delle Reti Elettriche nasce al fine di sviluppare uno strumento che consenta una gestione unificata della cyber security, di promuovere e realizzare iniziative di collaborazione, scambio informazioni e di ricerca nel settore delle Generazione, Trasmissione e Distribuzione dell'Energia Elettrica attraverso il coinvolgimento di partner pubblici e privati.

Il tavolo di lavoro permanente che si è formato nel 2015 svolge tuttora le proprie attività riguardanti le Infrastrutture Critiche Elettriche Nazionali a tutti i livelli del sistema nazionale Generazione, Trasmissione e Distribuzione (AT/MT/BT) con un'attenzione specifica ai nuovi assetti di Cyber Security della moderna rete Nazionale che presenta in numero sempre maggiore nodi di Generazione Green nonché alle moderne Smart-Grid/Micro-Grid (Generazione Distribuita).

La linea guida è rivolta alle aziende nazionali ed europee del settore elettrico, di piccole, medie o grandi dimensioni, suggerisce obiettivi e metodiche per affrontare le tematiche di cyber security, in modo integrato e allineato con il Framework NIS e il Framework Nazionale di Cyber Security, con le linee guida e gli standard internazionali; raccomanda inoltre la predisposizione dei più importanti controlli di sicurezza da implementare in stretto accordo con la supply chain.

Il primo sforzo è stato rivolto all'identificazione delle metodiche che consentano il coinvolgimento del Top Management, facilitando un linguaggio comune tra varie figure aziendali con diversi background e sensibilità sul tema, fino alla definizione di una metodica comune per presentare ai membri del Consiglio di Amministrazione tutti i rischi informatici correlati con l'Information Technology (IT) e l'Operational Technology (OT).

Si vuole inoltre suggerire come migliorare lo scambio delle informazioni, condividere 'best practices' al fine di contribuire ad una maggiore consapevolezza dell'impatto dei rischi cyber nelle aziende energetiche e nel settore energetico nel suo insieme.

Viene evidenziata la necessità che il settore debba adottare un approccio sistemico e valutare il problema attraverso il controllo dell'intera filiera, per migliorare i sistemi di protezione e limitare qualsiasi possibile effetto domino che potrebbe essere causato dal un guasto in un'area della catena di valore.

Nelle linee guida si vuole inoltre rafforzare la consapevolezza da parte degli operatori di quanto sia cruciale gestire il processo da un punto di vista di una corretta pianificazione della gestione della Continuità Operativa evidenziando come la resilienza del sistema rispetto alla sicurezza Cyber debba diventare parte integrante e imprescindibile del sistema di gestione stesso.

Voglio ringraziare sentitamente A2A, AIIC, ANSALDO ENERGIA, CERT NAZIONALE, CISCO, DELOITTE, ENEL, IREN, LEONARDO, PANTA RAY, KASPERSKY, TERNA che in collaborazione con la Scuola Politecnica dell'Università di Genova hanno permesso la realizzazione dalla prima edizione del documento.

Il Presidente dell'Osservatorio

Prof.ssa Paola Girdinio

INDICE

1. Introduzione e scopo del documento

Nel presente documento vengono esposte le linee guida per la Cyber Security nell'ambito dei sistemi elettrici, avendo come riferimento il framework NIST (National Institute of Standards and Technologies) e gli standard tecnici relativi allo specifico contesto. I primi capitoli includono spiegazioni utili anche ai livelli manageriali per meglio comprendere il contesto di rischio insieme alle raccomandazioni per mettere in atto le contromisure sia a livello organizzativo sia tecnico.

2. Cos'è la Cyber Security e il Contesto Normativo

Questa sezione introduttiva intende fornire esempi di incidenti Cyber accaduti nel settore e indicare quindi la conseguente importanza di implementare contromisure efficaci per contrastare il rischio cyber.

2.1. Introduzione

In riferimento al contesto industriale/energetico possiamo affermare che negli ultimi anni si è evoluto verso tecnologie sempre più moderne e digitali. In particolare l'ICT (Information and Communication Technology) sta ridisegnando la storia industriale delle infrastrutture strategiche. Attualmente, stiamo affrontando la quarta rivoluzione industriale che comprende una evoluzione/fusione tra gli ambiti delle reti IT e OT convergendo tecnologicamente verso l'Internet of Things (IoT). Perciò, con l'aumento dei dispositivi connessi verso la rete e in particolare l'arrivo delle applicazioni IoT, assieme alle diverse tecnologie e alla loro integrazione (come il Cloud Computing e i Big Data), seguiranno inevitabilmente una serie di problematiche quali l'interoperabilità, la sicurezza e l'affidabilità di una nuova generazione di infrastrutture strategiche/critiche.

Nello stesso tempo il settore elettrico ha vissuto e sta vivendo a tutt'oggi grandi evoluzioni. Infatti, la liberalizzazione del mercato sta imponendo un cambiamento delle fonti di generazione dell'energia stessa a favore delle rinnovabili e un livello di interconnessione sempre maggiore fra le reti elettriche; di conseguenza questo ha generato una proliferazione di operatori elettrici provenienti da un numero sempre maggiore di regioni/paesi.

All'interno di questa nuova realtà, maggiormente digitalizzata a livello sia nazionale sia europeo, la cybersecurity ha un ruolo molto importante ed è quindi sotto la lente attenta dei maggiori player dell'energia (Generazione, Trasmissione e Distribuzione), sia nazionali sia europei (futura prossima Super Grid Europea) e che fanno parte di un unico corpo delle infrastrutture critiche quali quelle elettriche, che devono tra l'altro garantire, su vari livelli di responsabilità, la fornitura di un servizio pubblico e una continuità di questo servizio essenziale per tutte le regioni/nazioni europee.

Gli standard Internazionali di riferimento, Incidenti e Contromisure fanno riferimento a normative tecniche e linee guida relative alla sicurezza dei sistemi di generazione - trasmissione - distribuzione dell'elettricità, si è potuto portare avanti azioni di analisi delle norme NIST (National Institute of Standards and Technologies), NERC (Natural Environment Research Council), NIS (Network and Information Systems), NISTIR (National Institute of Standards and Technology Interagency Report), IEC (International Electrotechnical Commission), ISO (International Organization for Standardization), CIP (Critical Infrastructure Protection).

Questa analisi è stata effettuata considerando i requisiti di Affidabilità, Integrità, Confidenzialità e Non Ripudio, specificati nelle varie normative.

E' emersa l'importanza di considerare la Cyber Security in modo multidisciplinare. Nei settori energetici, e nello specifico in quello elettrico, sono stati considerati i differenti ambiti dell'informatica, del networking, dell'automazione, del controllo di sistemi complessi (SCADA, IEDs, ICS, DCS, HMI, PLC, …).

Questa linea guida suggerisce la definizione e l'attuazione di un modello multi-livello di gestione della sicurezza, applicato ai sistemi di automazione, controllo e supervisione.

La trasformazione tecnologica dei sistemi energetici culminerà con l'affermazione dei cosiddetti sistemi cyber-fisici; infatti durante i vari incontri nel tavolo dell'Osservatorio Nazionale, si è argomentato come l'evoluzione dei sistemi stia giungendo a una prima affermazione dei sistemi cyber-fisici stessi, con conseguenti ripercussioni nella vita di tutti i cittadini che usufruiscono di servizi essenziali.

2.2. Esigenze specifiche di Cyber Security dei sistemi elettrici

Mentre ai sistemi IT si applicano i Critical Security Control (adattati dal SANS) nonché il Framework NIST, i sistemi cyber-fisici (CPS) necessitano di un insieme specifico di controlli di sicurezza, e il genere di protezione è amplificato dalla criticità dei sistemi stessi.

Inoltre l'ordine di importanza dei requisiti classici di Affidabilità, Integrità, Confidenzialità e Non Ripudio, è differente rispetto a quello dei sistemi IT nei quali prevale normalmente l'attenzione per la Confidenzialità dell'informazione.

Pertanto, le attività di analisi e valutazione dei rischi non possono limitarsi al solo Framework NIST, ma nei settori energetici devono necessariamente considerare anche altri framework di sicurezza. Volendo indicare quelli più significativi, ricordo: NERC-CIP, ISA, IEC, e chiaramente NIST per la protezione dei CPS.

Una chiara integrazione del Framework NIST è dovuta al bisogno di garantire la sicurezza e la resilienza dei sistemi di controllo industriale, e di assicurare la disponibilità e la massima affidabilità dei sistemi e delle procedure di safety.

L'esigenza di innalzare i livelli di sicurezza è dovuta anche alla progressiva introduzione di nuove tecnologie, sia energetiche, sia ICT (cloud computing, sistemi trasmissivi wireless, industrial IoT).

2.3. Aspetti generali

La trasformazione (complessa) dei sistemi energetici richiede nuovi approcci alla sicurezza delle reti e dei sistemi. A tale scopo, saranno necessarie le seguenti attività:

- analisi integrata dei rischi;
- analisi d'impatto valutazione dei rischi e delle minacce finalizzate alla tutela della continuità operativa;
- analisi dei rischi caratteristici, per tipologia di impianto/stabilimento;
- valutazione e gestione dei rischi di sicurezza fisica;
- valutazione e gestione dei rischi dei vendor tecnologici;
- valutazione e gestione dei rischi delle terze parti (fornitori di prodotti e servizi);
- adozione di modelli di gestione integrata dei rischi.

2.4. Precedenti requisiti e interessi

Il fronte delle esigenze può essere riassunto in questo elenco degli ulteriori requisiti riscontrati, durante la recente analisi delle normative, delle linee guida, delle raccomandazioni:

- requisiti di sicurezza delle comunicazioni nelle piattaforme di automazione e controllo basate sul modello Smart Grid;
- requisiti di sicurezza (safety e security) di impianti e sistemi di produzione delle energie rinnovabili;
- requisiti di sicurezza delle risorse energetiche distribuite (DER - Distributed Energy Resource);
- requisiti di sicurezza degli smart meter elettrici.

2.5. Principali azioni di rafforzamento della cybersecurity

Queste sono alcune delle principali azioni di rafforzamento attuabili, comunicate di recente a livello internazionale:

- impiego di ulteriori capacità di protezione fisica degli impianti (sicurezza integrata);
- sviluppo e adozione di capacità di misurazione dei livelli di disponibilità e sicurezza dei sistemi di controllo degli impianti;
- sviluppo e adozione di capacità di monitoraggio delle reti elettriche di trasmissione e distribuzione;
- sviluppo e adozione di capacità di monitoraggio della disponibilità dei sistemi di trasmissione;

- sviluppo e adozione di capacità di rilevamento e segnalazione degli incidenti di sicurezza;
- test di verifica dei livelli di robustezza del networking;
- test di verifica dei livelli di affidabilità dei dispositivi IIoT installati;
- test di verifica dei livelli di prontezza e adeguatezza dei piani di difesa informatica/cyber.

3. Un approccio alla Cyber Security per il settore elettrico

Questa sezione è dedicata al management aziendale. Intende fornire una panoramica di alto livello su come gestire il Cyber Risk nelle infrastrutture critiche di ambito elettrico.

3.1. Il ruolo del Top management nella gestione del rischio Cyber

Le imprese sono sempre più oggetto di sofisticate tecniche di attacco e per questo motivo hanno cominciato a dotarsi di risorse tecnologiche e finanziarie sempre più rilevanti per migliorare la propria protezione. Le minacce riguardano tutte le imprese, le grandi ma anche le medie e le piccole sono diventate potenziali bersagli, per la presenza di significativi asset immateriali e un livello di protezione inferiore i danni non sono esclusivamente legati al furto di proprietà intellettuale, ma anche alla reputazione dell'azienda. È sempre più frequente che a causa di attacchi, alcuni dirigenti perdano la propria posizione. Le sempre più diffuse regole di Corporate Governance impongono che i dirigenti siano responsabili della conduzione e protezione delle proprie attività. Per i motivi su esposti, è necessario che i Consigli di Amministrazione e il top management di aziende/istituzioni/organizzazioni comprendano e valutino i nuovi rischi, bilanciando la crescita e la profittabilità di mercato con la tutela dell'azienda e la mitigazione dei rischi. Tale compito è già previsto nel mandato del Consiglio di Amministrazione che, anche attraverso il Comitato Controllo e Rischi ove presente, è chiamato a definire la natura e il livello di rischio compatibile con gli obiettivi strategici dell'azienda, includendo nelle valutazioni tutti i rischi che possono assumere rilievo nell'ottica della sostenibilità nel medio-lungo periodo dell'attività dell'azienda. Inoltre, il Consiglio è anche chiamato a valutare l'adeguatezza dell'assetto organizzativo, amministrativo e contabile dell'azienda. Tali principi sono ad esempio già contenuti nel codice di autodisciplina di Borsa Italiana. Non vi è dubbio che il rischio cyber debba essere valutato come potenziale "rischio principale" per le aziende e le organizzazioni pubbliche, come evidenziato nella Relazione Annuale 2014 della Presidenza del Consiglio dei Ministri sulla politica per la Sicurezza della Repubblica.

Non vi è dubbio che, vista la portata e gli effetti della minaccia cyber, questa debba rientrare tra i rischi di alto rilievo che oramai ogni azienda e organizzazione deve valutare e gestire. Nell'ambito dell'attuazione di questi principi di Corporate Governance e in linea con le indicazioni contenute nel Quadro Strategico e nel Piano Nazionale, le aziende dovrebbero avviare le iniziative/pratiche a livello di Consiglio di Amministrazione e top management di seguito indicate.

3.1.1. La cybersecurity come elemento strategico nelle politiche di governance aziendale

La Governance aziendale si riferisce all'insieme di regole, di ogni livello (leggi, regolamenti etc.) che disciplinano la gestione e la direzione di un'azienda (o più in generale di un'organizzazione, sia essa pubblica o privata) e include le relazioni tra i vari attori coinvolti (gli stakeholder) e gli obiettivi dell'organizzazione stessa. Gli attori principali sono gli azionisti (shareholder), il consiglio di amministrazione (board of director) e il management. Più in generale, il governo di un'organizzazione abbraccia una serie di regole, relazioni, processi e sistemi aziendali, tramite i quali l'autorità fiduciaria è esercitata e controllata. La struttura della governance aziendale esprime quindi le regole e i processi con cui si prendono le decisioni in un'azienda, le modalità con cui vengono decisi gli obiettivi aziendali nonché i mezzi per il raggiungimento e la misurazione dei risultati raggiunti.

Tutte le aree di un'azienda contribuiscono a stilare le linee guida che consentono di definire la governance dell'organizzazione e in tal senso, anche la cybersecurity deve essere considerata in un'ottica di visione sistemica condivisa per cui la cyber non sia vista come elemento posticcio o di disturbo, bensì sia integrata come uno degli aspetti fondamentali nella definizione dei rischi, ergo sia considerata uno degli elementi strategici intorno ai quali si estrinseca la visione aziendale.

Il top management predispone dunque un piano di governo integrato della cybersecurity che coinvolga tutte le

funzioni aziendali e che includa tutte le aree di rischio operativo, definendo chiaramente i ruoli e le responsabilità e la loro opportuna separazione (principio della segregazione dei compiti) che individui tre livelli di controllo: controllo di primo livello, sotto la responsabilità diretta di chi opera la funzione (produzione, IT, vendite, ecc.); controlli di secondo livello, sotto la responsabilità di una funzione di sicurezza, esterna alle funzioni di produzione/business; controlli di terzo livello, sotto la responsabilità delle funzioni di controllo interno (audit). La funzione responsabile dei controlli di secondo livello dovrà occuparsi di definire le politiche di sicurezza aziendale e verificarne la loro corretta applicazione (compliance). Inoltre, il top management si assicura che il piano di governo integrato risponda alle seguenti esigenze:

- fornisca un allineamento tra la gestione del rischio e gli obiettivi strategici dell'azienda;
- definisca l'indicazione degli intervalli di tempo - approvate dal top management - per la determinazione delle conseguenze di una interruzione nella fornitura di prodotti e servizi.
- definisca un modello organizzativo che fornisca una copertura dei processi e domini di sicurezza di tutta l'azienda;
- definisca, nel modello organizzativo, un processo di gestione integrata del rischio al fine di inquadrare e contestualizzare, valutare, rispondere e monitorare i rischi relativi all'organizzazione e ai suoi asset, servizi, individui, altre organizzazioni e allo Stato;
- allochi in modo efficiente ed efficace le risorse richieste da una gestione sistemica aziendale, inclusa la gestione dei rischi;
- definisca un processo di monitoraggio e reportistica dell'efficacia ed efficienza organizzativa (secondo le metriche desiderate e condivise con il top management) nonché un processo di gestione del cambiamento nel caso di esigenza di modificare la propria struttura aziendale, avvalendosi di opportuni approcci di analisi (es. System Dynamics) che tengano in considerazione la dinamicità e la "sistemicità" intrinseche dell'organizzazione;
- fornisca, in tale processo, una misurazione, monitoraggio e presentazione del processo di gestione dei rischi.

Il top management si assicura che il modello di governo e il piano di cybersecurity siano integrati con il piano aziendale per la gestione dei rischi (Enterprise risk management) e il piano di gestione crisi o "crisisplan". Sempre più frequentemente gli impatti derivati dalla minaccia cyber sono classificabili come crisi e pertanto è indispensabile una gestione coerente e integrata, eventualmente avvalendosi di strumenti e metodologie di supporto alle decisioni che forniscano un'ottica integrata del modello di sistema e considerino tutte le dinamiche aziendali (es. Model-based Governance). Tra gli aspetti che vengono portati all'attenzione del top management vi sono anche quelli relativi alla gestione del rischio nel caso di contratti di outsourcing e cloud. Spesso si crede erroneamente che vi sia cessione del rischio, ma non è così: vi è solo una modalità diversa di gestione operativa della sicurezza, che richiede attente valutazioni da parte sia del top management sia del CISO e delle strutture coinvolte nella gestione del servizio.

3.1.2. Ruoli e responsabilità

Una corretta Governance aziendale deve essere integrata ossia deve avere una visione olistica e condivisa dal proprio management delle interdipendenze tra le varie funzioni aziendali e degli impatti che alcune problematiche in una di tali funzioni potrebbero provocare a cascata su altre. La stessa Governance deve prevedere la definizione di un corretto assetto organizzativo che includa un processo di miglioramento continuo sia nei propri processi sia nelle proprie policy e dunque l'abbattimento di modelli mentali errati da parte dei responsabili di funzione, tendendo così a quella che viene virtuosamente definita una Learning Organization. Ad esempio, è ormai noto che alcune strategie di aggressione di tipo sociale (attraverso il multiforme fenomeno noto come Insider Threat) si sono dimostrate particolarmente efficaci per aggirare controlli marcatamente tecnologici a discapito di procedure di sicurezza relative all'introduzione di materiali informatici esterni all'azienda, oppure attraverso la dissimulazione di personale di servizio esterno (come nel noto caso del Mall Target, negli USA). La cybersecurity è una tematica che tocca dunque tutta l'azienda, dal top management alle strutture operative, e deve essere pertanto soggetta a una valutazione sistemica e a un monitoraggio continuo. Nelle aziende spesso si pensa che sia sufficiente assegnare la gestione della cybersecurity in maniera esclusiva alla struttura ICT, senza il coinvolgimento delle aree di business. Sebbene l'ICT ricopra un ruolo centrale nella gestione della sicurezza, questa impostazione è incompleta e presenta alcuni possibili problemi; ne elenchiamo alcuni:

- il rischio cyber viene visto principalmente da un punto di vista dei sistemi informativi, fornendo spesso contromisure inadeguate;
- si assume implicitamente che vi sia una limitata coniugazione tra le esigenze del business e la riduzione dei rischi di tutta l'organizzazione;
- si introducono difficoltà organizzative intrinseche nell'implementare processi e contromisure di sicurezza all'interno delle varie funzioni aziendali (di business, di produzione, amministrative, ecc);
- vi è una parzialità dei piani di gestione della sicurezza;
- possibile tensione tra investimenti ICT e investimenti di sicurezza (non di rado, tagli ai budget ICT ricadono direttamente sui budget di cybersecurity).

Al fine di garantire una copertura completa dell'azienda, sarebbe opportuno affiancare le funzioni di sicurezza che si trovano all'interno della divisione ICT, con funzioni di sicurezza "logica" collocate al di fuori dell'ICT (solitamente a riporto del Chief Security Officer o del Chief Risk Officer, oppure in alcuni casi a riporto diretto del Direttore Generale, del Chief Operating Officer o dell'Amministratore Delegato). Questa funzione di sicurezza logica è guidata dal CISO - Chief Information Security Officer. Questa impostazione garantisce i principi di segregazione delle responsabilità, nonché consente di poter differenziare i controlli di sicurezza di primo livello (a carico dell'ICT o delle funzioni di business/produzione) dai controlli di secondo livello (a carico del CISO e/o della funzione di sicurezza logica).

3.1.3. Il ruolo del CISO

La figura del Chief Information Security Officer o CISO è individuata dal top management, che si accerta che il ruolo sia assegnato a persona con adeguate competenze ed esperienza in materia. Tra le responsabilità del CISO vi dovrà essere:

- Avviamento/evoluzione di un piano di gestione dei rischi informatici aziendali, è quindi necessario che rischio venga approcciato in modalità "Enterprise", secondo i principi di ERM (Enterprise Risk Management), ad esempio secondo lo standard ISO31000
- Monitoraggio dell'evoluzione dei rischi e conseguente adeguamento del piano
- Analisi dei maggiori incidenti, delle loro conseguenze e delle azioni intraprese per la mitigazione di future occorrenze
- Relazione periodica al top management
- Funzione di raccordo tra il top management, le funzioni aziendali e le istituzioni nazionali ed estere.

Nelle aziende di medie/grandi dimensioni, tale ruolo dovrebbe essere assegnato a figura dedicata a questo scopo.

3.1.4. Monitoraggio integrato

Il top management valuta periodicamente i rischi individuati, di concerto con l'ERM complessivo, e il piano previsto per la loro mitigazione. Il top management è chiamato a esprimersi e decidere sulle scelte relative alle strategie di mitigazione/accettazione/cessione del rischio cyber, così come già avviene per tutti gli altri rischi a cui è esposta l'azienda.

3.1.5. Risorse

Il top management dovrà valutare se il piano di sicurezza sia correttamente supportato da adeguate risorse in termini economici e di personale chiamato a svolgere le attività inerenti. Le risorse allocate dovranno essere coerenti e in linea con il piano di gestione dei rischi aziendali (Enterprise risk management). L'eventuale rischio residuo dovrà essere correttamente valutato e se non in linea con le linee generali, si dovrà definire dei piani di trattamento del rischio, valutando l'opportunità di ridurre il rischio tramite applicazioni di contromisure, evitare il rischio, eliminando le sorgenti di questo rischio, oppure trasferire il rischio.

3.1.6. Consapevolezza e cultura della cybersecurity

Il top management dovrà condurre attività per promuovere la consapevolezza e la cultura della cybersecurity

a tutti i livelli aziendali. Il CISO predisporrà un programma per aumentare la consapevolezza del personale interno ed esterno al fine di ridurre i rischi derivati da uso improprio o errato degli strumenti e dei processi informativi dell'organizzazione. Inoltre, potranno essere previste esercitazioni interne e/o di settore e nazionali per testare e migliorare la capacità del top management e delle strutture operative di gestire eventi cyber.

3.1.7. Scambio di informazioni e cooperazione

Il top management dovrà promuovere e supportare iniziative finalizzate a stabilire e rafforzare rapporti di cooperazione con altre organizza zioni dello stesso settore e con gli organi istituzionali deputati al contrasto della minaccia cyber. L'adesione a CERT di Settore o CERT a carattere istituzionale (come il CERT Nazionale) e la cooperazione con altre organizzazioni permette di migliorare la comprensione della minaccia, la condivisione di pratiche e strumenti di contrasto e, in alcuni casi, di poter sviluppare capacità comuni.

3.2. Il Top Management nel Governo del Rischio: codice di autodisciplina di Borsa Italiana, regole di Corporate Governance

La cybersecurity è un tema che deve trovarsi stabilmente sul tavolo degli organi di vertice dell'Azienda, che devono garantire il giusto commitment su tutta la filiera gerarchica e operativa affinché siano perseguiti gli obiettivi di resilienza e presidio degli asset informativi. Ma quale deve essere il ruolo del vertice su una tematica che rischia continuamente di essere derubricata a "problema tecnologico" cui dare una risposta tecnologica?

Le direttrici di indirizzo e di azione sono essenzialmente quattro:

- Indirizzo della strategia cyber: il vertice aziendale, in maniera analoga a quanto viene fatto per altri rischi corporate, deve indirizzare la strategia di cybersecurity indicando l'attitudine al rischio cyber che l'azienda intende mantenere (risk appetite framework - RAF) , in relazione ai principali scenari di impatto, quali possono essere il danneggiamento di sistemi di business, la perdita di riservatezza o di disponibilità di informazioni chiave fino ad arrivare agli impatti sui sistemi di OT (Operations Control) come ad esempio i sistemi di controllo industriale (ICS - Industrial Control System o SCADA - Supervisory Control and Data Acquisition). Di conseguenza i vertici delle singole business unit declineranno la strategia cyber in precisi obiettivi di sicurezza sulle informazioni e sui sistemi, fornendo quelle valutazioni che consentiranno, sui tavoli tecnici, di definire profili di sicurezza allineati alle esigenze e in grado di bilanciare i costi (sia economici sia operativi) con una adeguata riduzione del rischio cyber.
- Assicurare che governance e reporting siano in linea con la strategia di cybersecurity e rispettate da tutti. L'elemento centrale della governance resta il corpo delle Politiche di Sicurezza, che stabilisce le regole su cui si articola la strategia di cyber defence, su cui si innesta il Piano Strategico della Cybersecurity, documento programmatico che declina gli obiettivi di sicurezza, unitamente alle risorse e tempi per conseguirli. Il reporting, che nelle realtà maggiormente evolute potrà essere integrato con quello di altri rischi di business, dovrà avere una duplice natura: da un lato fornire lo stato delle difese e l'efficacia delle misure di protezione in atto, dall'altro dovrà misurare il raggiungimento degli obiettivi di piano strategico in termini di tempi, costi e qualità.
- Promozione dell'Awareness:
    - Awareness del Top Management
    - Awareness dei Business Owner
    - Awareness degli stakeholders interni ed esterni (inclusa supply chain)
- Promuovere i comportamenti in linea con le pratiche di sicurezza, evitando di incorrere in prima persona in quelle pratiche che possono costituire falle nelle difese aziendali. Comportamenti quali la cessione delle credenziali di accesso personali allo staff, l'utilizzo di posta elettronica o cloud privato per il forward o la memorizzazione di informazioni aziendali, l'uso di social o sistemi di messaggistica istantanea (whatsapp) per la comunicazione di informazioni riservate, devono essere evitati in quanto possono dar luogo a emulazione lungo tutta la filiera gerarchica, aumentando la probabilità di attacchi cyber.

4. La Cyber Security nel sistema di gestione della business continuity e del rischio

L'ultima edizione del documento Horizon Scan Report - pubblicato con cadenza annuale dal Business Continuity Institute - dimostra che tra le principali preoccupazioni dei Business Continuity Manager figurano un attacco cyber (88%) e una minaccia di data breach (81%). Lo stesso Cyber Resilience Report - pubblicato ogni anno dal medesimo istituto - ha rivelato come il 66% delle organizzazioni sia stato colpito da un incidente di tipo cyber almeno una volta negli ultimi 12 mesi e addirittura il 15% ha subito oltre 10 attacchi.

Appare chiaro quindi come il tema stia assumendo una rilevanza sempre crescente per i professionisti che si occupano di continuità operativa e gestione del rischio, quali discipline tese a garantire la resilienza dell'organizzazione.

Il settore energetico - e in particolare gli operatori elettrici - non fanno eccezione. Il mondo sta diventando sempre più digitale e con esso anche le minacce che ci troviamo ad affrontare. Diventa quindi fondamentale, in un'ottica di attenta pianificazione per la continuità operativa e di corretta gestione dei rischi, lavorare per la resilienza dell'organizzazione in caso di evento critico di natura cyber.

In relazione ai nuovi scenari di rischio e alla crescente complessità dell'attività di erogazione dell'energia elettrica, caratterizzata da un intenso utilizzo della tecnologia dell'informazione, gli operatori elettrici devono quindi predisporre dei Sistemi di Gestione della Continuità Operativa e del Rischio in grado di assicurare la continuità delle proprie funzioni e in particolare dell'erogazione di energia anche a fronte di eventi critici di tipo cyber potenzialmente in grado di determinare interruzioni.

La continuità operativa è intesa come la capacità degli operatori elettrici di continuare a erogare il servizio a livelli predefiniti accettabili a seguito di un incidente. Il campo di applicazione del Sistema di Gestione della Continuità Operativa prevede riflessioni, oltre che sull'ambito informatico e tecnologico, anche su persone, siti, risorse e fornitori dell'organizzazione. A tali fini, si consiglia agli operatori elettrici di nominare un *Responsabile del Programma di Continuità Operativa* (cosiddetto *Business Continuity Manager*) e di definire un Sistema di Gestione della Continuità Operativa (cosiddetto *Business Continuity Management System*).

Nello specifico, gli operatori elettrici sono incoraggiati a definire, attuare e mantenere in ottica di miglioramento continuo:

- una politica organizzativa di continuità operativa e di gestione del rischio che stabilisca il campo di applicazione e il modello di governance dei rispettivi Sistemi di Gestione, anche attraverso la nomina di persone competenti e l'impegno dei vertici dell'organizzazione nello sviluppo costante di una capacità di prevenzione e risposta a eventi critici di tipo cyber;
- un programma di formazione e sensibilizzazione continuo delle risorse finalizzato a incorporare la continuità operativa, la gestione del rischio e la cybersecurity nella cultura organizzativa;
- una business impact analysis che identifichi, qualifichi e quantifichi gli impatti nel tempo di un'interruzione sull'organizzazione al fine di classificare i processi critici in base all'urgenza di ripristino. Un'analisi dei requisiti di continuità che quantifichi e qualifiche le risorse necessarie a recuperare l'attività dopo un'interruzione e un'analisi delle minacce che identifichi eventuali singoli punti di cedimento e concentrazioni inaccettabili di rischio (con particolare riferimento alle minacce di tipo cyber);
- soluzioni di continuità operativa e misure di mitigazione delle minacce cyber che siano sempre coerenti con gli scopi dell'organizzazione;
- un piano di continuità operativa costantemente aggiornato, che rappresenti l'insieme di procedure documentate atte a guidare l'organizzazione nel rispondere, recuperare, riprendere e ripristinare a un livello predefinito le attività a seguito di un'interruzione di tipo cyber. Tipicamente, il piano copre le risorse, i servizi e le attività richieste per assicurare la continuità delle funzioni organizzative critiche;
- un piano di disaster recovery costantemente aggiornato, che costituisce parte integrante di quello di continuità operativa di cui sopra e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione;
- un programma annuale di esercitazioni e test finalizzati ad allenare la risposta dell'organizzazione a un evento critico di tipo cyber e a individuare i limiti dei piani nell'ottica di garantire il miglioramento continuo del Sistema di Gestione.

L'Internal Audit dovrà poi verificare e riferire periodicamente (almeno una volta all'anno) al Consiglio di

Amministrazione in merito all'adesione dell'organizzazione ai seguenti Standard internazionali di riferimento:

- ISO 22301:2012 Societal security -- Business continuity management systems -- Requirements;
- ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements;
- ISO 31000:2009 Risk management – Principles and guidelines.

4.1 La Business Impact Analysis (BIA)

La **Business Impact Analysis** (**BIA**) è il processo di analisi delle attività di un'organizzazione e degli effetti che un'interruzione potrebbe avere su di esse. La BIA costituisce il fondamento su cui viene costruito un programma di Business Continuity Management e serve a identificare, quantificare e qualificare gli impatti nel tempo di un arresto dei processi di un'organizzazione. La Business Impact Analysis fornisce inoltre i dati utili per la determinazione di appropriate strategie di continuità, mediante la classificazione dei processi critici in base all'urgenza di ripristino.

Sebbene non vi sia un'unica modalità di riferimento per la raccolta dei dati nell'ambito di una BIA, i professionisti che intendono affrontare un processo di questo tipo per la prima volta o in maniera ricorrente all'interno di un Sistema di Gestione dovrebbero considerare:

- Il campo di applicazione del programma di Business Continuity Management e il perimetro dei processi critici dell'organizzazione, da stabilire all'inizio della BIA;
- Le indicazioni degli intervalli di tempo – approvate dal Top Management – per la determinazione delle conseguenze di una interruzione nella fornitura di prodotti e servizi;
- L'impatto di un'interruzione nel tempo, al fine di dare una base oggettiva al Top Management per determinare le urgenze nel recupero dei processi critici;
- La necessità di utilizzare una metodologia che sia coerente e omogenea in tutta l'organizzazione, per garantire che vi sia comparabilità tra i processi analizzati, e che sia sufficientemente robusta, in modo da limitare la componente soggettiva e assicurare che i responsabili di processo non enfatizzino eccessivamente o minimizzino l'urgenza delle loro attività.

Inoltre, è di fondamentale importanza per la buona riuscita della Business Impact Analysis che siano raccolti esclusivamente dati rilevanti e pertinenti, che gli impatti vengano determinati in maniera sufficientemente realistica (pur con la consapevolezza che non possono essere calcolati con estrema precisione) e che non si cada nella tentazione di ponderare gli impatti di un'eventuale interruzione per la probabilità di accadimento di un ipotetico evento critico. La BIA **non è**, infatti, un'analisi di rischio.

La **ISO TS 22317:2015,** che rappresenta lo Standard internazionale di riferimento in materia di Business Impact Analysis, propone un approccio metodologico ben preciso composto da una serie di fasi che - se sviluppate correttamente - consentono di ottenere dei risultati molto utili per la selezione di strategie e tattiche di continuità operativa che siano coerenti con gli scopi dell'organizzazione.

I prerequisiti per una buona BIA, innanzitutto, includono:

- La definizione ex-ante di un perimetro di analisi, che sia coerente con il campo di applicazione del programma di Business Continuity Management;
- La definizione e la comunicazione di ruoli e responsabilità chiare per lo sviluppo delle analisi di impatto, valutazione dei rischi e delle minacce finalizzate alla tutela della continuità operativa.
- L'ottenimento di un mandato alto, che dimostri l'impegno del Top Management verso il progetto di BIA;
- Lo stanziamento di risorse adeguate, che consenta anche la formazione delle risorse coinvolte nel processo sugli aspetti specifici relativi alla BIA.

A questo punto, è possibile effettuare una prima riflessione sulla Business Impact Analysis con l'obiettivo di:

- Identificare i prodotti e servizi prioritari, su cui indagare nel dettaglio gli impatti in caso di interruzione;
- Determinare le categorie di impatto (tipicamente economico/finanziario, commerciale, legale/regolamentare e reputazionale) e le relative soglie di criticità;
- Selezionare le fonti più appropriate per la raccolta delle informazioni;

- Organizzare interviste, workshop e questionari per la raccolta dei dati.

Questa fase preliminare è tipicamente detta BIA Iniziale e serve anche a stabilire il Maximum Tolerable Period of Disruption (MTPD) dell'organizzazione.

Successivamente, si procede con l'analisi degli impatti vera e propria esclusivamente per il perimetro di prodotti/servizi, processi e attività critici individuato in fase di BIA iniziale. L'analisi viene svolta su più livelli:

- **Per i Prodotti e Servizi**, con l'obiettivo di delineare un MTPD per ciascun gruppo di prodotti/servizi, stabilire il Minimum Business Continuity Objective (MBCO) e definire una bozza di Recovery Time Objective (RTO);
- **per i Processi**, con l'obiettivo di delineare un MTPD per ciascun gruppo di processi che concorrono all'erogazione dei prodotti/servizi critici, stabilire il Minimum Business Continuity Objective (MBCO) per i processi in oggetto e definire una bozza di Recovery Time Objective (RTO) e di Recovery Point Objective (RPO);
- **per le Attività**, con l'obiettivo di confermare i sopra citati parametri a livello di attività e raccogliere i requisiti di continuità in termini di persone, siti, risorse e fornitori. La Business Impact Analysis a questo livello analizza e raccoglie anche le informazioni relative ai requisiti di continuità (risorse, siti, tecnologia, attrezzature, fornitori ecc.).

A valle della raccolta dei dati è importante prevedere una fase di consolidamento dei risultati che consenta di comparare i processi critici per diversi livelli di urgenza. Il consolidamento è fondamentale per selezionare delle strategie e delle tattiche di continuità operativa che siano coerenti con gli obiettivi dell'organizzazione.

Gli obiettivi di una Business Impact Analysis sono:

- Documentare gli impatti che nel tempo deriverebbero da un'interruzione;
- Identificare il massimo periodo tollerabile per un'interruzione o arresto (Maximum Tolerable Period of Disruption - MTPD);
- Determinare le priorità di un'organizzazione per il recupero dei propri processi critici;
- Identificare le dipendenze e le risorse (sia interne sia esterne) necessarie a raggiungere i livelli di servizio (Service Level Agreement - SLA) concordati.

Nello specifico, per Maximum Tolerable Period of Disruption (MTPD) si intende il tempo che impiega un impatto avverso in grado di interrompere l'erogazione di un prodotto/servizio o di un'attività a diventare inaccettabile, mettendo cioè a rischio la sostenibilità stessa dell'organizzazione.

4.2 La gestione dei rischi e l'evoluzione verso il Dynamic Risk Management

Come anticipato nei capitoli precedenti, le organizzazioni sono oggi chiamate a fronteggiare scenari costantemente in evoluzione di rischi cyber. La prima cosa da definire è cosa sia un rischio: un rischio è l'effetto dell'incertezza su un obiettivo (ISO Guide 73:2009). Sotto questa definizione del rischio è evidente che un rischio può rivelare anche risvolti positivi: in questo caso si parla di opportunità. Ai fini di questa linea guida tratteremo solamente rischi intesi come eventi con potenziale risvolto negativo.

È poi lecito chiedersi cosa sia un rischio nel mondo cyber: un rischio nel mondo cyber è un evento potenziale legato alla perdita di confidenzialità, integrità o disponibilità di dati o informazioni a valle del quale potrebbero derivare impatti negativi sull'organizzazione, a persone, altre organizzazioni o, cosa particolarmente rilevante per la presente linea guida, a livello di sistema paese.

I rischi nel mondo cyber sono generati dall'incontro di vulnerabilità di sistemi o elementi che li costituiscono, con una minaccia (threat) che è in grado di sfruttare quella vulnerabilità specifica, determinando un impatto.

Così come fornire una definizione di rischio, è essenziale definire cosa sia una minaccia: una minaccia è definita come "la causa potenziale di un avvenimento indesiderato, che può provocare danni agli individui, a un sistema o a un'organizzazione" (ISO 22300:2012).

Diventa quindi evidente il livello di complessità del tema e la conseguente necessità di definire un approccio strutturato per consentire l'analisi dei rischi cyber in termini di individuazione, misurazione, gestione e monitoraggio degli stessi per agevolare l'assunzione di decisioni consapevoli da parte dell'organizzazione.

Attraverso una corretta analisi del rischio è quindi possibile individuare le principali criticità, vulnerabilità e

potenziali contromisure da mettere in campo per ridurre l'esposizione al rischio su gli ambienti mission critical.

Sono presenti in letteratura molteplici esempi di metodologie e approcci per la gestione dei cyber risk, (es. NIST 800-30, ISO27005, IRAM2) che identificano tutte almeno una serie di step essenziali comuni:

- Identificazione dell'ambito di intervento e del contesto, in cui dovrà essere valutato il perimetro aziendale di processi critici interesse, il contesto cyber in cui il perimetro identificato è inserito, il livello di dettaglio in termini di elementi target rispetto ai quali eseguire le attività di risk assessment che consentono di erogare i processi critici;
- Esecuzione di risk assessment, in cui saranno identificati i rischi cyber, le contromisure per rischio in essere, e una valutazione quantitativa o qualitativa del livello di rischio sul target analizzato;
- Identificazione dei piani di trattamento dei rischi o accettazione, in cui dovranno essere definite le azioni di mitigazione, trattamento o trasferimento del rischio, incluse contromisure, specifiche o compensative, polizze assicurative o altri strumenti di trasferimento del rischio nonché eventuali razionali per accettazione del rischio residuo;
- Monitoraggio o revisione dei rischi, in cui periodicamente o su base di specifici eventi trigger come, ad esempio, cambiamenti nelle strategie aziendali (es. in una situazione di insourcing, si decide di migrare le applicazioni in ambiente Cloud) saranno eseguite attività di revisione sul livello di rischio e avanzamenti sullo stato di implementazione dei piani di trattamento;
- Comunicazione dei rischi e consultazione, in cui per ogni valutazione fatta saranno identificati gli stakeholder necessari per una corretta valutazione e i rischi identificati saranno comunicati alle specifiche funzioni responsabili.

Il risultato finale sarà quello di identificare, valutare e monitorare, per tutti i rischi cyber identificati, il livello di **rischio inerente** (rischio all'istante iniziale senza la presenza di alcuna contromisura, il **rischio residuo attuale** (rischio residuo allo stato attuale considerando le misure già in essere) e **rischio residuo futuro** (rischio residuo a seguito dell'implementazione in futuro di uno o più controlli identificati per ridurre il livello di rischio a un valore accettabile per l'azienda).

I rischi sono sempre valutati sul confronto tra il livello residuo attuale e l'attitudine al rischio dell'azienda. I rischi che superano il livello di attitudine al rischio dell'azienda, saranno gestiti con l'obiettivo di ridurre il rischio a un livello accettabile o accettati.

Vale la pena evidenziare che il risk appetite non è un elemento proprio della tematica cyber ma deve essere valido per tutti i rischi gestiti dall'azienda.

Infatti, per una gestione dei rischi cyber di successo, è necessario che il rischio cyber sia trattato al pari degli altri rischi aziendali e portato all'attenzione del CCR (Comitato Controllo Rischi) o del BoD (Board of Director), per consentire ai vertici aziendali una valutazione coerente di tutti i possibili rischi a cui l'azienda è esposta e la conseguente gestione degli investimenti necessari per indirizzare azioni di mitigazione, riduzione o trasferimento. A tal fine è necessario che tutti i rischi siano rappresentati e presentati in maniera uniforme: il rischio cyber quindi, dovrà essere rappresentato nello stesso modo di rischi strategici, finanziari, etc.

Uno strumento estremamente efficace per perseguire questo risultato è quello di allineare il processo di cyber security risk management all'Enterprise Risk Management (di seguito ERM). L'ERM è il processo aziendale attraverso il quale per tutte le tipologie di rischio sono definite le modalità di rappresentazione e formalizzato il risk appetite dell'organizzazione e che struttura le attività di identificazione, valutazione e trattamento dei rischi.

Al fine di presentare tutti i rischi cyber al CCR o al BoD in un unico formato per ottenere una rappresentazione univoca dei rischi aziendali che evidenzi la comparazione dei livelli di rischio cyber con gli altri rischi gestiti a livello ERM, è necessario utilizzare una metodologia comune e integrata che consenta di analizzare i rischi aziendali in funzioni di impatti su una scala unica per tutta l'azienda e di parametri riconosciuti e in accordo con l'ERM aziendale.

La scelta della specifica metodologia di riferimento per la gestione dei rischi cyber e della granularità degli elementi su cui eseguire la valutazione, potrà poi essere determinata in funzione del corrente livello di maturità aziendale in tema di gestione dei rischi e dalla complessità del contesto di applicazione.

Mentre per la scelta della metodologia però, come anticipato, sono disponibili molte fonti di valore internazionale a cui attingere, per la granularità, la scelta dovrà essere estremamente ponderata e calata sullo

specifico contesto aziendale.

L'identificazione dell'elemento minimo da valutare, e cioè la granularità, dovrà essere coerente sia per elementi del mondo IT che per elementi del mondo OT, garantendo un livello di dettaglio affine per poter effettuare delle valutazioni di rischio comparabili e presentabili sullo stesso piano al CCR.

In linea generale sarebbe ragionevole pensare di valutare il rischio in funzione dell'elemento di base di tutti i sistemi digitali, siano essi IT o OT: il dato.

Tuttavia effettuare delle valutazioni del rischio su ogni dato è non sono complesso perché prevede un'attività di censimento di tutti i dati e dei percorsi che il dato segue all'interno e all'esterno della propria infrastruttura, ma genererebbe anche un numero di valutazioni decisamente troppo elevato. Si rende quindi necessaria l'individuazione di elementi della dimensione corretta; a titolo puramente esemplificativo si potrebbero considerare come elementi su cui eseguire le attività di analisi del rischio cyber, applicativi in ambito IT e sistemi afferenti a specifiche zone (in linguaggio IEC62443) del processo produttivo in ambito OT. Nel caso del mondo elettrico, la suddivisione in zone è piuttosto ragionevole in considerazione della estrema eterogeneità del contesto (per esempio, in ambito Generation, le diverse sorgenti avranno caratteristiche e peculiarità distinte, per la Trasmissione si considererà una realtà geograficamente estesa con canali di comunicazione di lunghezza notevole mentre per la Distribuzione si dovrà tenere in considerazione una maggiore capillarità sul territorio ma in aree più localizzate).

La valutazione di rischio dovrà essere svolta periodicamente per ogni singolo target identificato e la responsabilità per l'esecuzione delle attività di valutazione dovrà essere in carico alla funzione centrale con responsabilità di cyber security a livello aziendale (es. CISO), in qualità di Risk Owner sui temi cyber.

Per poter correttamente quantificare un rischio i parametri fondamentali da determinare risultano due: impatto e probabilità. Il rischio è infatti definito come $R = I \times P$.

Il tema della valutazione degli impatti è già discusso ampiamente nel capitolo relativo alla continuità operativa.

Per quanto riguarda la probabilità invece, è opportuno fare alcune considerazioni per il caso specifico del mondo cyber:

- la probabilità è considerata relativa al successo di un evento cyber avverso. Questo perché un tentativo di attacco non riuscito, non è un rischio in quanto non avrebbe impatto;
- la probabilità è direttamente correlata alla possibilità di accadimento di un evento cyber e alle vulnerabilità presenti nel sistema. Il tema della probabilità è estremamente complesso nel caso cyber perché da un lato esistono pochi dati storici sugli eventi cyber per la creazione di modelli di previsione matematica che riescano a individuare in modo affidabile la frequenza di accadimento di tali eventi e dall'altro ogni elemento connesso a una rete può essere oggetto di attacchi cyber da parte di un numero molto elevato di minacce;
- La probabilità è in generale tanto più bassa quanto minori sono le vulnerabilità e queste ultime sono essere collegate alle minacce (non tutte le minacce possono sfruttare tutte le vulnerabilità).

Per ridurre le vulnerabilità è necessario implementare delle contromisure, che possono essere mutuate dai controlli definiti da standard internazionali - es. SANS (System Administration, Networking, and Security Institute), CSC per il mondo OT, IEC 62443, IEC 62351 per il mondo OT. I controlli, infatti, indirizzano la scelta di contromisure per specifiche aree tematiche relative al mondo della cyber security (Identity and Access Management, Event detection e Incident Response, etc.). Le contromisure dovranno poi essere declinate in funzione delle specifiche minacce che sono ritenute rilevanti per l'azienda.

Per ottenere informazioni relative alla probabilità e agli impatti quindi, si consiglia che il Risk Owner per i rischi cyber si coordini con le figure responsabili di IT Security e OT Security e con i responsabili della continuità operativa per raccogliere le informazioni in merito agli impatti.

Un modello di gestione del rischio che contempli le minacce, dovrà tenere conto della variabilità nel tempo delle stesse, aggiornando dinamicamente i rischi cyber.

Un processo di inclusione delle minacce dinamiche all'interno del modello di valutazione del rischio si può strutturare in 5 fasi che prevedono:

- Monitoraggio fonti: in questa fase sono monitorate le informazioni provenienti da fonti aggiuntive quali Cyber Threat Intelligence, Enti Regolatori e Organizzazioni internazionali preventivamente

identificate. Le modalità e la frequenza di monitoraggio delle fonti è variabile in funzione della tipologia di elemento su cui la fonte fornisce informazioni (es. una sorgente di Cyber Threat Intelligence potrebbe produrre informazioni su base quotidiana, mentre un Ente Regolatore avrebbe un periodo di riferimento di mesi). È importante considerare che il contesto degli operatori elettrici a livello mondo è da anni all'avanguardia sul tema della gestione dei rischi cyber (si pensi alla normativa NERC CIP per il Nord America) e quindi il livello di maturità e affidabilità delle sorgenti di intelligence è piuttosto elevato;

- Identificazione: sulla base delle informazioni ottenute, bisognerà quindi identificare le minacce di interesse, sulla base di profili preventivamente definiti e validati e in funzione di uno specifico evento o trend associati a una minaccia cyber (la causa potenziale di un avvenimento indesiderato, che può provocare danni agli individui, a un sistema o a un'organizzazione" (Fonte: ISO 22300:2012)). di interesse. Ad esempio:
    - Campagna Ransomware nel settore elettrico
    - Aumento trend malware su sensori utilizzati per manutenzione predittiva (es. IIoT)
- Caratterizzazione: lo step successivo consiste nell'Identificazione della categoria e egli attributi associati all'evento. Questi sono definiti sulla base di modelli che tengano conto delle specificità delle variabili. Ad esempio la minaccia può essere caratterizzata in termini di attributi sulla base di Threat Model che prevedano la determinazione di parametri come:
    - Threat Entity Goal Orientation (attori, motivazione, interesse)
    - Threat Entity Capabilities (risorse, skill)
    - Threat Entity Modus Operandi
- Correlazione: in questa fase si procederà con la Correlazione degli attributi con gli elementi e i criteri di valutazione del rischio. La correlazione dovrà essere basata su tabelle/modelli di mappatura e logiche di aggiornamento. Gli attributi della minaccia sono poi collegati con i criteri di valutazione della probabilità di minaccia (e quindi delle contromisure presenti o da implementare) impiegata nella valutazione del rischio statico.
- Aggiornamento del rischio: l'ultimo passaggio è relativo all'Aggiornamento del livello di rischio e presentazione della variazione. La variazione della probabilità di minaccia determina un ricalcolo ed eventuale aggiornamento del livello di rischio e, a fronte di variazione, saranno determinate ulteriori azioni necessarie per il trattamento.

Rispetto alla gestione delle fonti e al relativo monitoraggio, è doveroso evidenziare che risulta difficilmente applicabile un'attribuzione di responsabilità agli specifici Risk Owner IT o OT. In questo caso potrà essere il CERT ad avere il compito di abilitatore del processo di gestione dinamica attraverso attività di raccolta e analisi delle fonti di intelligence al fine di individuare eventi di minaccia con impatto sugli elementi oggetto di valutazione del rischio e che avrà il ruolo di ingaggiare i responsabili della gestione del rischio.

5. Computer Emergency Readiness Team (CERT)

Nel contesto del settore elettrico, è sempre più importante definire un approccio integrato per prevenire e gestire gli incidenti di sicurezza cyber. L'obiettivo è di migliorare la "cyber readiness" ovvero la capacità di prevenire le minacce cyber in una maniera proattiva evitando, per quanto possibile, di avere impatti significativi sui dipendenti, sugli asset, sui servizi e, in generale, sulla competitività e reputazione dell'azienda.

Il CERT, da intendersi principalmente come un "Cyber Emergency Readiness Team", è la struttura che ha il mandato di realizzare questo approccio e di proteggere la propria "Constituency" assicurando un adeguato livello di servizio.

Per "Constituency", in ambito energia, si deve intendere non solo i dipendenti ma anche gli asset dell'azienda, comprendendo impianti di produzione, reti di distribuzione, edifici e tutto ciò che contribuisce alla fornitura del servizio, con particolare attenzione alle infrastrutture critiche e a quelle che erogano servizi essenziali.

Il modello funzionale del CERT consiste di diverse componenti chiave che sono supportate da un vasto insieme di tool, servizi e funzionalità che insieme consentono al CERT di soddisfare la sua missione e di raggiungere i propri obiettivi.

Tra gli aspetti importanti della missione di un CERT, in modo non esaustivo, si possono sicuramente elencare i seguenti:

- monitorare le occorrenze di incidenti cyber contribuendo al processo di miglioramento continuo dei controlli e delle contromisure di sicurezza informatica
- analizzare gli incidenti sia per mitigarne l'impatto sia per ridurre e limitarne le future occorrenze;
- coordinare la risposta agli incidenti informatici coinvolgendo sia gli attori interni all'azienda sia le controparti esterne (ad esempio i CERT nazionali);
- produrre la reportistica per le funzioni aziendali e il management interno;
- incrementare la cultura interna nel gestire gli incidenti di sicurezza attraverso simulazioni e esercitazioni.

Gli obiettivi del CERT devono essere legati non solo agli aspetti più tecnici, come può essere la riduzione del numero di incidenti, ma anche ad aspetti più "business" come la riduzione dell'impatto degli incidenti sugli asset, servizi, reputazione e competitività dell'azienda.

Questi obiettivi possono essere raggiunti attraverso:

- gestione, coordinamento, supporto e monitoraggio degli incidenti di sicurezza e del livello di maturità dei processi di prevenzione e di risposta;
- creazione e rinforzo di una "trusted community" all'interno dell'azienda e con le controparti esterne significative;
- attivazione di un canale con la funzione di comunicazione aziendale per gestire la comunicazione relativa agli incidenti sia verso l'interno che verso i media esterni;
- monitoraggio delle attività di "recovery" generate come follow-up degli incidenti di sicurezza;
- raccolta e condivisione delle informazioni relative a potenziali minacce per l'azienda, con una attenzione particolare alle minacce esterne che possono sfruttare debolezze interne.

I seguenti processi sono inclusi nel perimetro del CERT:

- **Risposta all'incidente**: è il processo chiave per prevenire, individuare, rispondere e ripristinare a fronte di incidenti di cyber security. Il processo deve essere realizzato con un approccio sistematico e strutturato in cui vi è una costante comunicazione tra gli attori interni e esterni e che prevede almeno le seguenti fasi:
  - "Preparedness and prevention"
  - "Detection"
  - "Analysis"
  - "Response"
  - "Recovery"

- **Monitoraggio delle minacce**: è il processo di raccolta e gestione delle informazioni "privilegiate" relative alle minacce cyber, ai relativi attori e vettori ed è chiave per prevenire e rispondere agli incidenti di sicurezza se si traducono queste informazioni in azioni utili e applicabili per evitare, mitigare o gestire i potenziali incidenti di sicurezza.
- **Condivisione delle informazioni**: è il processo per realizzare una comunicazione "trusted" tra i diversi attori coinvolti basato sui principi di "need-to-share" e "need-to-know".
- **Simulazioni di impatto** fatte sulla base della conoscenza delle minacce e vulnerabilità di cui dispone il CERT, al fine di comprendere in maniera preventiva la migliore strategia di difesa
- **Esercitazioni periodiche** (Cyber War Gaming e Red Teaming) per **addestrare** il personale, testare le procedure di risposta e misurare i risultati ottenuti al fine di valutare l'efficacia delle misure di prevenzione, risposta e ripristino.

6. Implementare contromisure nel contesto delle infrastrutture critiche in ambito elettrico

Le Infrastrutture Critiche relative ai sistemi elettrici si possono classificare secondo una gerarchia di dimensione e complessità molto varia:

- Grandi Impianti classici di generazione termici
- Sistemi di generazione Idroelettrici distribuiti

- Generazione rinnovabile distribuita (DER)
- Sistemi di trasmissione e distribuzione dell'energia (migliaia di sottostazioni primarie e centinaia di migliaia di sottostazioni secondarie).

I sistemi telecontrollati e i sistemi distribuiti fanno uso di infrastrutture e protocolli di telecomunicazione e pertanto sono esposti a tutti i rischi correlati a tale contesto, ma anche i grandi impianti non possono ormai essere operati in modo isolato: la sicurezza di sistemi, reti e protocolli è pertanto un elemento essenziale.

Le possibili minacce possono essere infatti veicolate tramite mezzi di natura non connessa come ad esempio media removibili o dispositivi ritornati dopo una manutenzione. Anche l'accesso ai sistemi da parte di personale esterno può costituire una ulteriore minaccia.

È necessario tenere conto delle differenti esigenze dei contesti fortemente centralizzati (come le Centrali Termiche), degli impianti Idroelettrici fortemente distribuiti e tutti telecontrollati e della generazione rinnovabile. Per ciascuno di questi ambiti è stato necessario pertanto sviluppare una opportuna e peculiare strategia.

Nel contesto dei sistemi industriali i sistemi possiedono un ciclo di vita ben più lungo di quello dei sistemi informatici. Pertanto è necessario collaborare con i costruttori per includere nei prodotti sin dall'origine anche le misure di sicurezza, ma anche applicare contromisure opportune per garantire la vita a sistemi informatici più datati.

La rete di telecontrollo delle reti di distribuzione rappresenta un ambito ancora più complesso poiché coinvolge centinaia di migliaia di sottostazioni primarie e secondarie, e ancora più granulare è l'infrastruttura del contatore elettronico. Man mano che ci si avvicina alle "foglie" del sistema l'ordine di grandezza degli oggetti cresce e con esso la necessità di individuare una specifica strategia per la sicurezza.

È necessario pertanto operare per quanto possibile con gli strumenti attualmente disponibili ma supportando anche lo sviluppo di soluzioni innovative, supportando gli enti normatori nello sviluppo delle versioni sicure dei protocolli di telecontrollo e automazione.

Il contrasto alle minacce di cybersecurity avviene mediante l'adozione di adeguate contromisure, denominate tecnicamente "controlli". Per controllo si intende pertanto un'azione di natura organizzativa o tecnica in grado di ridurre il rischio che la minaccia possa tradursi in un attacco di potenziale successo.

I controlli di sicurezza sono oggetto di continuo sviluppo e classificazione attraverso lo sviluppo di numerosi standard internazionali. Esistono pertanto alcuni "framework di sicurezza" che raggruppano i controlli secondo categorie e ambiti applicativi.

Il framework di riferimento adottato in questa linea guida è il "Framework for improving Critical Infrastructure Cybersecurity V1.0" – NIST - February 12 - 2014, con gli aggiornamenti della revisione V.1.1". Il framework NIST è basato su un approccio "risk based" nel senso che associa la priorità e il livello di adozione dei controlli di sicurezza al concetto di analisi del rischio, e si struttura nei seguenti componenti:

- **Framework Core:** un insieme di attività di Cyber Security, risultati desiderati e riferimenti applicabili alle infrastrutture critiche. I controlli di sicurezza descritti nel core framework sono classificati sulla base di cinque livelli (o ambiti) concorrenti alla realizzazione della sicurezza: Identify, Protect, Detect, Respond, Recover. Il nome di ciascun livello suggerisce in modo intuitivo la tipologia di controlli a cui farà riferimento e la sequenza in cui i livelli sono riportati è altrettanto indicativa. I controlli del Framework Core sono definiti in modo da essere in prima istanza generici, ma comunque riferiti anche a standard di applicazione specifici dei diversi contesti delle Infrastrutture Critiche (e.g. per il sistema elettrico)
- **Framework Implementation Tiers:** definiscono un metodo per valutare il livello di maturità (da Tier 1 a Tier 4) nell'applicazione dei controlli del Framework Core nell'ambito di una specifica organizzazione.
- **Framework Profile:** rappresenta il profilo di sicurezza che ogni organizzazione ha deciso di attuare anche sulla base delle esigenze di business e sui relativi requisiti di continuità in funzione dell'analisi del rischio. In realtà possono esistere più "profile" a seconda del contesto specifico, anche nell'ambito di una singola organizzazione. Inoltre i profile possono essere classificati come "corrente" o "obiettivo" con l'intento di individuare un percorso di miglioramento della postura di cybersecurity. In generale ogni profile comprende un insieme di controlli e la relativa maturità.

Le Framework Function sono dettagliate in categorie di controlli e ciascuno di questi ultimi in sottocategorie di controlli. L'ultima colonna contiene i riferimenti agli standard tecnici che consentono l'attuazione del controllo negli specifici contesti.

Bibliografia

- IEC 62351 - Power Systems Management and Associated Information Exchange – Data and Communications Security"
- IEC 62443 - Security for industrial automation and control systems"
- 2015 Italian Cyber Security Report, Un Framework Nazionale per la Cyber Security
- CYBERSECURITY, Critical Infrastructure. Framework for Improving Critical Infrastructure Cybersecurity. 2014.
    - HILDICK-SMITH, Andrew. Security for critical infrastructure scada systems. SANS Reading Room, GSEC Practical Assignment, Version, 2005, 1: 498-506.
- FORCE, JOINT TASK; INITIATIVE, TRANSFORMATION. Security and privacy controls for federal information systems and organizations. NIST Special Publication, 2013, 800: 53.
- STOUFFER, Keith; FALCO, Joe; SCARFONE, Karen. Guide to industrial control systems (ICS) security. NIST special publication, 2011, 800.82: 16-16.
- PCI DSS Standard.
- ISO/IEC 27001:2013 Standard.
- ISO/IEC 27002:2013 Standard.
- ISO/IEC 27005:2011 Standard.
- Business Continuity and Crisis Management:
    - ISO 22301:2012 Societal security -- Business continuity management systems – Requirements
    - ISO 22313:2012 Societal security -- Business continuity management systems -- Guidance
    - ISO/TS 22317:2015 Societal security -- Business continuity management systems -- Guidelines for business impact analysis (BIA)
    - ISO/TS 22318:2015 Societal security -- Business continuity management systems -- Guidelines for supply chain continuity
    - BS 11200:2014 Crisis Management. Guidance and good practice
    - "The BCI Good Practice Guidelines – 2018" issued by the Business Continuity Institute
    - "BCI How To Guides" issued by The Business Continuity Institute
- Risk Management:
    - ISO 31000:2009 Risk management – Principles and guidelines
    - ISO/IEC 31010:2009 Risk management -- Risk assessment techniques
- Organizational Resilience:
    - ISO 22316:2017 Security and resilience -- Organizational resilience -- Principles and attributes

Siti Web di riferimento

- Homeland Security - Cyber Security Publications: https://www.dhs.gov/cybersecurity-publications
- Business Continuity and Crisis Management:
    - The Business Continuity Institute: www.thebci.org
    - Disaster Recovery Institute: www.drii.org
    - Continuity Central: http://www.continuitycentral.com/
- Risk Management

- The Institute of Risk Management: https://www.theirm.org/
- Committee of Sponsoring Organizations (COSO) of the Treadway Commission: https://www.coso.org/

- Organizational Resilience
  - Horizon Scan Report, issued by the Business Continuity Institute (BCI): http://www.thebci.org/index.php/download-the-horizon-scan-2017
  - Cyber Resilience Report, issued by the Business Continuity Institute (BCI): http://www.thebci.org/index.php/obtain-the-cyber-resilience-report-2016

Fonti Principali

- NIS Directive, The Directive on security of network and information systems, adopted by the European Parliament on 6 July 2016 Directive (EU) 2016/1148;
- European General Data Protection Regulation (GDPR);
- NERC CIP (North American Electric Reliability Corporation critical infrastructure protection) Plan
- CONSEJO NACIONAL DE OPERACIÓN – CNO - Colombia Acuerdo 788 dated 03/09/2015;
- Ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas " from Spain Government – dated 28/04/2011;
- Ley 5/2014, de 4 de abril, de Seguridad Privada, regulate the performance and provision of private security activities and services;
- National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cyber Security", version 1.0 February 2014;
- Research Center of Cyber Intelligence and Information Security (Sapienza Università di Roma) e Laboratorio Nazionale CINI di Cyber Security (Consorzio Interuniversitario Nazionale per l'Informatica), "2015 Italian Cyber Security Report - Un Framework Nazionale per la Cyber Security", versione 1.0 Febbraio 2016.

Fonti Principali Recenti 2017/2018

- Council of European Energy Regulators (CEER)
- https://www.ceer.eu
- EURELECTRIC
- http://www.eurelectric.org
- European Network for Cyber Security (ENCS)
- https://encs.eu
- European Network of Transmission System Operators for Electricity (ENTSO-E)
- https://www.entsoe.eu
- EPRI
- https://www.epri.com
- SEPA - Smart Electric Power Alliance
- https://sepapower.org
- IEEE - Cybersecurity of Energy Delivery Systems
- http://www.ieee-ecce.org

- IEC - International Electrotechnical Commission
- http://www.gridstandardsmap.com/
- Interoperability Strategic Vision
- https://gridmod.labworks.org/sites/default/files/resources/InteropStrategicVision2017-04-11.pdf
- EU Commission Task Force for Smart Grids
- https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force.