Cyber Security e resilienza operativa del gruppo Dolomiti Energia

Dolomiti Energia Rinnovabili. Integrati. Indipendenti.

Indice

Dolomiti Energia Rinnovabili. Integrati. Indipendenti.

CYBER SECURITY E RESILIENZA OPERATIVA DEL GRUPPO DOLOMITI ENERGIA

1. Contesto e scenario di riferimento

L'evoluzione digitale intrapresa dal gruppo Dolomiti Energia negli ultimi anni ha determinato un progressivo e significativo incremento nell'utilizzo di strumenti e tecnologie informatiche a supporto dell'automazione dei processi aziendali. Questa trasformazione ha portato a una crescita esponenziale del numero di dispositivi connessi alla rete aziendale, tra cui personal computer, smartphone, tablet, nonché un'ampia gamma di sistemi di Operation Technology (OT), come ad esempio smart meter per la telelettura dei consumi energetici, sistemi SCADA per il controllo e la supervisione degli impianti industriali e piattaforme di gestione delle infrastrutture critiche.

A questa crescita infrastrutturale si affianca l'adozione di nuove tecnologie informatiche, tra cui il cloud computing, che consente una gestione più flessibile e scalabile delle risorse IT, e l'intelligenza artificiale, sempre più utilizzata per l'analisi predittiva, l'ottimizzazione dei processi e il supporto alle decisioni operative e strategiche. Parallelamente, l'introduzione di nuove modalità di lavoro, come lo smartworking e il lavoro ibrido, ha contribuito ad allargare e rendere sempre più labile il perimetro aziendale dal punto di vista informatico, estendendo la superficie di attacco ben oltre i confini fisici tradizionali delle sedi aziendali.

Questa evoluzione comporta un duplice effetto: da un lato incrementa l'esposizione del gruppo Dolomiti Energia ad attacchi di natura cyber, dall'altro amplifica l'impatto potenziale che tali attacchi possono avere sulla continuità dei servizi erogati alla collettività, sui processi gestionali interni e sulle operazioni industriali. Il Gruppo, in qualità di operatore attivo nei settori della produzione e distribuzione e vendita di energia elettrica e servizi a valore aggiunto, della distribuzione e vendita di gas naturale, di teleriscaldamento, del ciclo idrico e della gestione dei rifiuti, è consapevole che un'interruzione o una compromissione dei propri sistemi informatici potrebbe avere ripercussioni significative non solo sull'organizzazione, ma anche sul territorio e sulle comunità servite.

Parallelamente, il panorama delle minacce informatiche si è profondamente trasformato negli ultimi anni. Gli attacchi cyber sono diventati sempre più sofisticati dal punto di vista tecnologico, eterogenei nella loro natura e nelle modalità di esecuzione, spaziando da campagne ad ampio spettro — come ransomware e phishing massivo — a violazioni estremamente mirate e personalizzate verso specifici soggetti o infrastrutture obiettivo. Gli attori delle minacce includono oggi organizzazioni criminali strutturate, gruppi sponsorizzati da stati nazionali e attivisti digitali, rendendo il contesto di rischio sempre più complesso e dinamico.

2. Policy di Cyber Security

In considerazione di questo scenario in continua evoluzione, il gruppo Dolomiti Energia ha adottato una policy di Cyber Security di Gruppo, concepita come documento strategico e operativo di riferimento per l'intera organizzazione. Tale policy stabilisce in modo chiaro e strutturato i principi guida, i ruoli e le responsabilità organizzative, nonché i presidi tecnici e procedurali necessari per proteggere in modo efficace il patrimonio informatico aziendale, sia in ambito Information Technology (IT) che Operation Technology (OT), garantire la continuità nell'erogazione dei servizi essenziali e assicurare la piena conformità alle normative vigenti in materia di sicurezza delle informazioni e protezione dei dati.

3. Obiettivi Strategici

La policy di Cyber Security del gruppo Dolomiti Energia persegue i seguenti obiettivi strategici, considerati fondamentali per la tutela del patrimonio informativo e tecnologico dell'organizzazione:

- **Protezione di sistemi, dati e servizi critici**: garantire che tutti i sistemi informatici, le banche dati, le applicazioni e i servizi digitali del Gruppo siano adeguatamente protetti da minacce interne ed esterne, salvaguardando la loro funzionalità e la loro integrità nel tempo.
- **Garanzia dei principi fondamentali della sicurezza delle informazioni**: assicurare in modo costante e verificabile la disponibilità, l'integrità, la riservatezza, la verificabilità e l'accountability delle informazioni trattate attraverso i sistemi informatici del Gruppo, in conformità con le migliori pratiche e gli standard internazionali di riferimento.
- **Conformità normativa**: garantire il pieno rispetto delle normative applicabili in materia di sicurezza informatica e protezione dei dati, con particolare riferimento al Decreto Legislativo 231/2001 in tema di responsabilità amministrativa degli enti, al Regolamento Generale sulla Protezione dei Dati (GDPR – Regolamento UE 2016/679) e alla Direttiva NIS2 (Direttiva UE 2022/2555), recepita in Italia con il Decreto Legislativo 138/2024.
- **Promozione della cultura della sicurezza**: diffondere a tutti i livelli dell'organizzazione — dal management ai collaboratori operativi, fino ai fornitori e ai partner esterni — una cultura consapevole e responsabile della sicurezza informatica, attraverso programmi strutturati di formazione, sensibilizzazione e comunicazione interna.
- **Miglioramento continuo**: implementare e mantenere un modello di gestione della sicurezza informatica basato sulla valutazione sistematica del rischio (risk-based

approach) e orientato al miglioramento continuo delle misure di protezione, in coerenza con l'evoluzione del contesto tecnologico e delle minacce.

4. Principi Fondanti

La policy di Cyber Security del gruppo Dolomiti Energia si fonda su una serie di principi cardine che ne guidano l'applicazione e ne garantiscono l'efficacia nel tempo:

- **Allineamento strategico**: la gestione della sicurezza informatica è pienamente integrata e allineata con la strategia digitale complessiva del gruppo Dolomiti Energia, assicurando che gli investimenti e le iniziative in ambito cyber siano coerenti con gli obiettivi di business.
- **Gestione integrata IT/OT**: la sicurezza viene gestita in modo integrato su entrambi i domini — Information Technology e Operation Technology — riconoscendo la crescente convergenza tra sistemi informativi tradizionali e sistemi di controllo industriale e la necessità di un approccio unificato alla protezione.
- **Adozione di framework riconosciuti**: il modello di gestione della sicurezza è basato sul Framework Nazionale per la Cybersecurity e la Data Protection, articolato nelle cinque funzioni fondamentali — Identify, Protect, Detect, Respond, Recover — che forniscono un approccio strutturato e completo alla gestione del rischio cyber.
- **Conformità agli standard internazionali**: i presidi tecnici e organizzativi adottati dal Gruppo sono coerenti con i principali standard internazionali di riferimento.

5. Presidi di Sicurezza

La policy definisce un insieme completo e articolato di controlli di sicurezza, progettati per coprire tutti gli ambiti rilevanti della protezione informatica:

- **Asset management e classificazione delle informazioni**: inventario degli asset informatici (hardware, software, dati) e classificazione delle informazioni in base alla loro criticità e sensibilità, al fine di applicare misure di protezione proporzionate al livello di rischio.
- **Controllo degli accessi**: implementazione di meccanismi di controllo degli accessi basati sul principio del minimo privilegio (least privilege) e sull'autenticazione a più fattori (MFA), garantendo che ogni utente possa accedere esclusivamente alle risorse strettamente necessarie allo svolgimento delle proprie attività.
- **Formazione e awareness**: programmi strutturati e continuativi di formazione e sensibilizzazione rivolti a tutto il personale del Gruppo, con l'obiettivo di sviluppare e mantenere un elevato livello di consapevolezza sui rischi informatici e sulle corrette pratiche di sicurezza.
- **Sicurezza fisica**: misure di protezione fisica dei locali che ospitano infrastrutture critiche, data center e apparecchiature di rete, inclusi sistemi di controllo degli accessi fisici, videosorveglianza e protezione ambientale.
- **Gestione dei sistemi**: un approccio strutturato alla gestione dell'intero ciclo di vita dei sistemi informatici, che comprende la progettazione sicura (security by design), la gestione tempestiva delle patch e degli aggiornamenti di sicurezza, le procedure di backup e disaster recovery, la segmentazione e la sicurezza delle reti e il monitoraggio continuo attraverso il Security Operations Center (SOC).
- **Incident management**: processi formalizzati e documentati per la rilevazione, l'analisi, la risposta e la notifica degli incidenti di sicurezza informatica, in piena aderenza ai requisiti previsti dal GDPR in materia di data breach e dalla Direttiva NIS2 in materia di notifica degli incidenti significativi.
- **Gestione dei fornitori**: un framework strutturato per la gestione della sicurezza nella catena di fornitura, che prevede requisiti di qualifica e contrattuali specifici in materia di cybersecurity, nonché controlli periodici e audit per verificare il mantenimento nel tempo degli standard di sicurezza richiesti.

6. Campo di applicazione

La policy di Cyber Security si applica in modo trasversale e vincolante a tutti gli utenti del Gruppo — dipendenti, collaboratori, consulenti e personale esterno — ai fornitori di servizi e prodotti informatici, nonché a tutti i sistemi di Information Technology (IT) e di Operation Technology (OT) delle Società del Gruppo sottoposte a direzione e coordinamento di Dolomiti Energia.

L'applicazione della policy si fonda sui seguenti principi operativi:

- **Conformità contrattuale e normativa**: rispetto di tutti i requisiti contrattuali e cogenti applicabili, con particolare attenzione alla protezione delle informazioni trattate nell'ambito del patrimonio informatico aziendale e alla tutela dei dati personali.
- **Gestione per processi**: strutturazione della gestione dei servizi informatici (IT/OT) attraverso un approccio per processi, che consente una visione organica e integrata delle attività di sicurezza e ne facilita il monitoraggio e il miglioramento.
- **Definizione di ruoli e responsabilità**: chiara definizione dei ruoli e delle responsabilità di tutti gli utenti in materia di cybersecurity, accompagnata dalla diffusione e dalla promozione attiva della cultura della sicurezza informatica a ogni livello dell'organizzazione.
- **Processo di escalation e segnalazione**: definizione di un processo strutturato di escalation che consenta a tutti i dipendenti e collaboratori di segnalare tempestivamente eventuali incidenti di sicurezza, vulnerabilità individuate o attività sospette, favorendo una risposta rapida e coordinata.
- **Responsabilizzazione e addestramento del personale**: coinvolgimento attivo e responsabilizzazione di tutto il personale attraverso programmi di formazione e addestramento specifici, finalizzati a sviluppare competenze pratiche nella prevenzione e nella gestione delle minacce informatiche.
- **Sicurezza dei sistemi e delle informazioni**: garanzia della sicurezza dei sistemi IT/OT, dei servizi da essi erogati e delle informazioni elettroniche, sia all'interno dell'organizzazione che negli scambi con terze parti esterne, attraverso la classificazione dei dati e l'attribuzione delle relative responsabilità agli utenti coinvolti.
- **Controllo degli accessi e prevenzione**: sviluppo e implementazione di contromisure organizzative e tecniche finalizzate a controllare l'accesso alle informazioni da parte degli utenti interni e delle terze parti, prevenendo accessi non autorizzati e mitigando il rischio di perdita, danneggiamento, furto, sabotaggio o compromissione dei dati e dei servizi informatici aziendali.
- **Eccellenza tecnologica**: garanzia di un livello costantemente elevato delle soluzioni tecnologiche adottate e in fase di implementazione, al fine di supportare efficacemente

il business del gruppo Dolomiti Energia e assicurare un vantaggio competitivo duraturo nel tempo, in linea con i piani di sviluppo strategico e i progetti approvati.

- **Continuità operativa**: prevenzione delle anomalie dei processi e dei servizi IT, protezione dei processi aziendali critici da guasti, avarie o disastri di rilievo dei sistemi informatici, e garanzia della loro tempestiva ripresa attraverso piani di continuità operativa e disaster recovery.
- **Protezione dei servizi essenziali**: tutela della sicurezza e della disponibilità dei servizi erogati agli utenti e alla collettività, con particolare riguardo ai servizi ritenuti essenziali ai sensi delle Direttive e dei Regolamenti vigenti in materia di sicurezza delle reti e dei sistemi informativi.
- **Gestione efficace degli incidenti**: gestione tempestiva, strutturata e efficace degli eventi e degli incidenti di sicurezza informatica, attraverso processi di identificazione rapida, contenimento delle conseguenze, analisi approfondita delle cause e implementazione di azioni correttive volte a ridurre la probabilità di accadimento futuro.
- **Monitoraggio e indicatori di prestazione**: definizione di obiettivi misurabili e monitorabili nel tempo attraverso indicatori di prestazione (KPI) specifici, che consentano di valutare l'efficacia delle misure di sicurezza adottate e di orientare le decisioni di investimento e miglioramento.
- **Ottimizzazione ed efficienza economica**: ottimizzazione continua dei processi di sicurezza per garantire la protezione dei servizi informatici gestiti, assicurando al contempo la migliore sostenibilità possibile delle soluzioni tecnologiche implementate, in un'ottica di efficienza e valorizzazione degli investimenti.
- **Miglioramento continuo**: attivazione e mantenimento di un sistema strutturato di miglioramento continuo, basato su cicli periodici di valutazione, revisione e aggiornamento delle misure di sicurezza, in risposta all'evoluzione del contesto tecnologico, normativo e delle minacce.

7. Azioni e risultati

Il modello di gestione della sicurezza delle informazioni adottato dal gruppo Dolomiti Energia si basa su normative internazionali e nazionali di riferimento e sulla valutazione continua e sistematica del rischio informatico, che consente di identificare, prioritizzare e trattare le minacce in modo proporzionato alla loro rilevanza e al potenziale impatto sull'organizzazione.

Nel corso del **2024** il Gruppo ha avviato il percorso di adeguamento alla Direttiva NIS2 (Direttiva UE 2022/2555), entrata in vigore nell'ottobre 2024 e recepita nell'ordinamento italiano attraverso il Decreto Legislativo 138/2024. Questo percorso rappresenta un impegno strategico significativo, volto a rafforzare ulteriormente la postura di sicurezza del Gruppo e ad assicurare la piena conformità ai nuovi requisiti normativi europei.

Nel corso del **2025** le attività di rafforzamento della sicurezza informatica sono proseguite e si sono intensificate in modo significativo:

- **Adeguamento NIS2**: è proseguito con regolarità il percorso di adeguamento alla Direttiva NIS2, rispettando tutte le scadenze previste dal quadro normativo e dalle indicazioni dell'Agenzia per la Cybersicurezza Nazionale (ACN).
- **Aggiornamenti infrastrutturali**: sono stati effettuati importanti aggiornamenti tecnologici alle architetture di sicurezza perimetrale, rafforzando le difese contro le minacce provenienti dall'esterno e migliorando la capacità di ispezione e filtraggio del traffico di rete.
- **Controllo degli accessi**: sono state aggiornate e potenziate le politiche e le architetture di controllo degli accessi alle reti del Gruppo, implementando soluzioni avanzate di autenticazione e segmentazione per ridurre la superficie di attacco interna.
- **Security Operations Center (SOC)**: sono stati rivisti e significativamente ampliati i servizi erogati dal Security Operations Center, potenziando le capacità di monitoraggio, correlazione degli eventi e risposta agli incidenti in tempo reale.
- **Attack Surface Monitoring**: sono stati potenziati i servizi di monitoraggio della superficie di attacco esterna (Attack Surface Monitoring), consentendo una visibilità più completa e tempestiva sulle potenziali esposizioni e vulnerabilità del Gruppo verso l'esterno.
- **Cyber Threat Intelligence**: sono state prese in carico e gestite in modo strutturato le segnalazioni generate dalle piattaforme OSINT (Open Source Intelligence) e CTI (Cyber Threat Intelligence), integrando queste informazioni nei processi decisionali e operativi di sicurezza.
- **Simulazioni e test di sicurezza**: sono state condotte simulazioni di attacco informatico, analisi approfondite di vulnerabilità e penetration test su sistemi e

applicazioni critiche, al fine di identificare e correggere proattivamente eventuali debolezze prima che possano essere sfruttate da attori malevoli.

- **Attività di Red Team**: sono state effettuate attività di Red Team, ovvero simulazioni avanzate di attacco condotte da team specializzati con l'obiettivo di testare in modo realistico la resilienza complessiva dell'organizzazione. Da queste attività sono scaturite iniziative di formazione specifica mirata per i team coinvolti.
- **Campagne di phishing simulato**: sono state condotte campagne di phishing simulato estese a tutta la popolazione aziendale, con l'obiettivo di misurare e migliorare il livello di consapevolezza dei dipendenti rispetto alle tecniche di ingegneria sociale più diffuse.
- **Security awareness e formazione**: è proseguita e si è intensificata l'attività di security awareness, erogata sia attraverso la piattaforma di e-learning aziendale sia attraverso contenuti pubblicati sulla intranet del Gruppo. È inoltre proseguita l'iniziativa di formazione frontale in ambito cybersecurity dedicata ai nuovi colleghi in fase di onboarding, assicurando che ogni nuovo ingresso nell'organizzazione riceva fin da subito le conoscenze fondamentali in materia di sicurezza informatica.
- **Audit e gestione fornitori**: sono stati effettuati audit mirati e attività strutturate di gestione del rischio dei fornitori, verificando il rispetto dei requisiti di sicurezza contrattualmente previsti e identificando eventuali aree di miglioramento nella catena di fornitura.
- **Audit interni/esterni**: sono stati condotti audit interni ed esterni approfonditi sui processi ICT e sulla sicurezza dei dati, al fine di verificare l'efficacia dei controlli in essere e individuare opportunità di rafforzamento.