FONDAZIONE BRUNO KESSLER
MAGAZINE

Dalla compliance alla resilienza: come cambia la sicurezza digitale nelle imprese

25 Marzo 2026

Con il supporto di InnovAction, il caso di Tecnoenergia Srl affronta le sfide della direttiva NIS2 tra strategia e operatività

Per le imprese che operano in ambiti critici come quello energetico, rafforzare la sicurezza digitale è oggi una priorità strategica oltre che normativa. All'interno del progetto InnovAction, negli ultimi mesi del 2025, si è svolta un'importante collaborazione tra il Centro per la Cybersicurezza della Fondazione Bruno Kessler (FBK) e Tecnoenergia Srl – un'azienda italiana con sede a Trento specializzata in servizi e soluzioni per il settore energetico e infrastrutturale. **Una realtà che opera nella gestione, manutenzione e telecontrollo di impianti energetici**, con un focus particolare sulle centrali idroelettriche e sui sistemi di produzione di energia da fonti rinnovabili.

InnovAction è un'iniziativa co-finanziata dal Ministero delle Imprese e del Made in Italy (MIMIT), al fine di costruire un Polo Europeo di Innovazione Digitale per supportare la trasformazione digitale e green delle aziende. Nello specifico, la Fondazione Bruno Kessler, con i suoi centri Cybersicurezza e Industria digitale, ha proposto servizi di "Test Before Invest" in varie aree operative consultabili nel catalogo disponibile qui. Nel caso specifico di Tecnoenergia, l'intervento ha superato la semplice verifica sperimentale, configurandosi come un percorso di definizione e validazione dei processi di governance della sicurezza L'obiettivo primario consisteva nel preparare la documentazione e le procedure necessarie a pianificare il futuro adeguamento alla **Direttiva NIS2** dell'azienda, non solo dal punto di vista normativo ma anche operativo, e cogliere l'opportunità' di rafforzare la propria postura di sicurezza.

La direttiva NIS2 è stata approvata dall'Unione Europea nel 2023 e rappresenta un'evoluzione della precedente direttiva NIS, emanata nel 2016. Il suo obiettivo principale è quello **innalzare il livello di protezione informatica in tutta Europa, uniformando le regole per ridurre i rischi legati ai cyber attacchi, ai furti di dati e alle interruzioni dei servizi essenziali**. La nuova versione della NIS2 amplifica notevolmente l'ambito di applicazione, coinvolgendo non solo settori critici come energia e trasporti, ma anche comparti come manifatturiero, alimentare, gestione rifiuti e pubblica amministrazione. Per una realtà che gestisce servizi essenziali come il telecontrollo di impianti attivi 24 ore su 24 per la produzione di energia, l'adeguamento alla direttiva

NIS2 **non è solo un obbligo normativo, ma un passaggio chiave per garantire continuità operativa e resilienza**.

Dall’analisi del rischio alla strategia

Il punto di partenza del percorso è stato la mappatura degli **asset strategici** e la conseguente valutazione dei rischi. Gli asset, nel contesto della sicurezza informatica e operativa, sono definiti come tutte le risorse, tecnologie, informazioni e infrastrutture che contribuiscono al funzionamento e al valore di un’organizzazione. Possono includere sistemi hardware, software, dati, processi aziendali, risorse umane e ogni elemento che supporta l’attività operativa e la continuità del business. Prima di definire qualsiasi contromisura, il gruppo di lavoro ha condotto un’analisi approfondita per identificare le vulnerabilità all’interno delle infrastrutture tecnologiche (IT) e operative (OT). Questa fase ha permesso di far emergere criticità latenti che, se ignorate, avrebbero potuto compromettere l’intera catena del valore. Si è trattato di un lavoro di analisi che ha distinto le criticità degli asset “accettabili” da quelli “non accettabili”. In questo contesto, sono stati definiti accettabili gli asset il cui rischio residuo rientra nei limiti di tolleranza aziendale, mentre i non accettabili sono quelli che presentano vulnerabilità tali da richiedere interventi prioritari di mitigazione, fornendo alla direzione di Tecnoenergia una fotografia delle priorità di intervento. Solo partendo da questa base di conoscenza della superficie d’attacco è stato possibile elaborare la documentazione necessaria per la compliance NIS2, come il Piano di Risposta agli Incidenti e l’analisi dei divari (Gap Analysis) rispetto allo standard ISO 27001.

Integrare operatività e compliance

La sfida principale è stata quella di armonizzare le esigenze di un’azienda dinamica con la rigidità dei requisiti normativi. Il problema si è configurato come un esercizio di ingegneria gestionale: integrare la velocità operativa richiesta dal business con i protocolli formali di sicurezza. Il progetto ha risposto a questa necessità non solo attraverso l’identificazione dei rischi tecnici, ma anche lavorando sulla definizione di ruoli e responsabilità nei momenti decisionali critici. L’adozione della Matrice RACI, uno strumento molto utilizzato in project management, ha infatti permesso di eliminare le ambiguità sui ruoli, assegnando responsabilità chiare per ogni processo di sicurezza. Parallelamente, per mitigare i rischi derivanti dall’esterno, è stato applicato il Modello di Kraljic, che aiuta a ragionare sul rischio di approvvigionamento e l’impatto sul business, alla sicurezza della catena di fornitura, permettendo di classificare i fornitori non solo in base al costo ma anche al loro impatto strategico sulla resilienza aziendale.

Un linguaggio comune

La difficoltà maggiore emersa dall’esperienza sul campo è stata quella di allineare linguaggi e prospettive differenti. Spesso l’approccio pragmatico dell’impresa, focalizzata sulla risoluzione immediata dei problemi operativi, deve confrontarsi con la necessità di formalizzazione richiesta dalla compliance alla NIS2. Viceversa, concetti astratti come “rischio residuo” o “maturità di gestione” devono tradursi in azioni concrete al fine di creare una ricaduta operativa concreta sulla postura di sicurezza dell’azienda. La chiave del successo è stata la capacità di adattarsi reciprocamente ovvero far convergere l’obbligo normativo con la realtà quotidiana dell’azienda. Il risultato è un framework di governance che non rallenta l’operatività, ma **la supporta e la rafforza, riducendo l’esposizione a rischi legali e operativi**.

Valore per il territorio

Per il Centro per la Cybersicurezza, il progetto ha rappresentato l’opportunità di applicare metodologie avanzate di risk management in un contesto reale di infrastruttura critica, validando modelli teorici su scenari concreti di integrazione IT/OT. Per l’azienda, il valore aggiunto supera quello di avere a disposizione una buona base per sviluppare la documentazione di conformità. Tecnoenergia dispone oggi di una strategia e di una roadmap definita per raggiungere una “maturità gestita” entro i termini della NIS2.

LINK

https://magazine.fbk.eu/it/news/dalla-compliance-alla-resilienza-come-cambia-la-sicurezza-digitale-nelle-imprese/

TAG

- #cyberattacchi
- #cybersicurezza
- #energia
- #fonti rinnovabili
- #green
- #idroelettrico
- #industriadigitale
- #innovaction
- #innovazione digitale
- #mimit
- #risk management
- #trasformazione digitale

AUTORI

- Martina Cicaloni