

Verso una elettrificazione cyber-safe

Nell'era della trasformazione digitale, la **cyber security** assume un ruolo fondamentale per garantire l'operatività delle imprese.

Le tipologie di attacchi informatici sono cambiate drasticamente negli ultimi anni: il numero è cresciuto in modo esponenziale, così come il loro grado di sofisticazione e impatto, per queste ragioni è sempre più difficile identificarne tempestivamente la fonte. Studi di settore confermano che la percezione del rischio cyber è in costante crescita. Rispetto agli anni precedenti, le cause dell'aumento degli attacchi informatici includono anche tensioni geopolitiche. Il conflitto tra Russia e Ucraina ha infatti aumentato l'attenzione in questo senso. In particolare, tutte le agenzie di sicurezza statali hanno messo in guardia Istituzioni pubbliche e private da potenziali minacce informatiche contro le infrastrutture critiche.

Nel 2022 molti degli attacchi più rilevanti a livello globale sono stati effettuati sfruttando la catena di fornitura e la compromissione di terze parti, consentendo agli attaccanti di colpire clienti, partner e fornitori del target primario; in questo modo è notevolmente aumentato il numero delle vittime e gli attacchi sono passati sempre più inosservati, realizzando il cosiddetto "scale effect". È interessante osservare, inoltre, che la maggior parte degli attacchi al settore energetico include quelli di tipologia ransomware, una modalità sempre più diffusa che determina l'esfiltrazione (copia, trasferimento o recupero non autorizzati) dei dati della vittima e la cifratura degli stessi, offrendo ai responsabili dell'attacco un'ulteriore leva per riscuotere il pagamento del riscatto.

Si osserva, inoltre, come le vulnerabilità rilevate nei prodotti software di ampio utilizzo siano in costante aumento e come queste vengano sfruttate sempre più rapidamente dai "criminali" informatici. In particolare, le vulnerabilità di tipo zero-day rappresentano un grande rischio perché vengono scoperte prima che gli sviluppatori di software ne vengano a conoscenza e prima che possano rilasciare un aggiornamento correttivo (patch).

In un simile contesto di cyber-warfare, l'unica difesa possibile è data da processi e tecnologie, messi a punto ed evoluti nel tempo e volti a mitigare il rischio informatico. Oltre alla costante applicazione della strategia di cyber security, abbiamo quindi previsto specifiche misure straordinarie, anche volte a rafforzare la "cyber security posture"⁽⁵⁾, consapevoli del fatto che il rischio cyber, nel complesso e interconnesso settore elettrico, assume proporzioni diverse, divenendo un rischio di portata ecosistemica. In tale scenario, per esempio, un blackout su larga scala avreb-

be ramificazioni socio-economiche tra famiglie, imprese e istituzioni vitali.

Elemento chiave diventa quindi la condivisione e la cooperazione sui temi di cyber security tra tutti gli stakeholder, siano essi aziende, organi legali o di controllo, fornitori, clienti o dipendenti.

Politiche e modello di gestione

In linea con le esigenze del settore industriale energetico e in coerenza con l'approccio strategico Open Power che lo caratterizza, abbiamo adottato una visione sistemica dei temi della cyber security, nonché una strategia globale di analisi, prevenzione e gestione degli eventi di sicurezza informatica. Il percorso della cyber security a supporto della trasformazione digitale del Gruppo si basa sulla definizione, valorizzazione e adozione di un modello di governance, infrastrutture e servizi di sicurezza, al fine di sfruttare al meglio le opportunità disponibili, anche coadiuvate da tecnologie all'avanguardia, per aumentare la resilienza informatica di infrastrutture e applicazioni.

Da settembre 2016, all'interno della Funzione Global Digital Solutions è stata costituita l'unità di **Cyber Security**, a diretto riporto del Chief Information Officer (CIO), e il cui responsabile ricopre il ruolo di Chief Information Security Officer (CISO) del Gruppo. L'unità è impegnata a garantire la governance, la direzione e il controllo delle tematiche di cyber security, la definizione della strategia, delle policy e delle linee guida, in conformità con le normative nazionali e internazionali, il supporto di ingegneria per la protezione degli ambienti del Gruppo, il monitoraggio della "risk posture" mediante controlli basati su processi e tecnologia, e ancora il presidio e l'attuazione dei requisiti di compliance derivanti da normative in tema di cyber security, unitamente all'adozione delle soluzioni tecniche e di procedure volte alla mitigazione di possibili debolezze rilevate. L'unità lavora in sinergia con le Linee di Business e con le unità tecniche responsabili della progettazione e gestione dei sistemi, grazie alle figure dei Cyber Security Risk Manager e dei Cyber Security Response Manager. Il CISO e i Cyber Security Risk Manager costituiscono inoltre il Cyber Security Operating Committee, che ha lo scopo di valutare trasversalmente il rischio cyber e ha l'obiettivo di definire i criteri di accettazione del rischio, in base alla "risk posture" di Gruppo. Il Cyber Security Committee, presieduto dal CEO di Gruppo e composto dalle sue prime linee, approva la strategia di sicurezza informatica e controlla periodica-

(5) Per "Cyber Security Posture" si intende lo stato di adozione da parte della società dei principi di sicurezza informatica.

mente i progressi della sua attuazione. Il Comitato, come stabilito nell'incontro di aprile 2021, si riunisce con cadenza semestrale; nel 2022 si sono tenuti due incontri (maggio e ottobre).

Il 2022 è stato caratterizzato, inoltre, da 3 incontri del Comitato Controllo e Rischi con l'obiettivo di approfondire aspetti legati alle procedure organizzative (sia a livello tecnico sia di governance), al processo di crisis management, al modello operativo del CERT e ai relativi processi che lo caratterizzano.

Tutte le aree partecipano attivamente all'attuazione della strategia di cyber security attraverso un piano operativo integrato e allineato agli obiettivi del Gruppo. Inoltre, la strategia e le iniziative di cyber security sono oggetto di costante approfondimento dei principali board esecutivi e di controllo (per esempio, Board of Directors, Organismi di Vigilanza ecc.) per tutte le legal entity e i Paesi di presenza del Gruppo.

Attraverso la policy di Gruppo adottata nel 2017, il **"Cyber Security Framework"**, si indirizzano, inoltre, i principi e i processi operativi che sono a supporto di una strategia globale di analisi, prevenzione e gestione dei rischi.

Tale Framework, basato su una visione 'sistemica', è trasversalmente applicabile al più tradizionale settore dell'Information Technology (IT), così come agli ambienti di Operational Technology (OT), legati al mondo industriale, e dell'Internet of Things (IoT). Nell'ambito dell'applicazione del Framework, nel 2017 è stata definita anche la metodologia di Cyber Security Risk Management, anch'essa applicabile a tutti gli ambienti IT, OT e IoT, che racchiude tutte le fasi necessarie per effettuare l'analisi dei rischi e definire il relativo piano di mitigazione, in coerenza con gli obiettivi di cyber security stabiliti. Per bilanciare i vantaggi ottenuti dall'operatività e dall'uso dei sistemi IT/OT/IoT con il rischio che da questi può potenzialmente derivare, sono infatti fondamentali decisioni ben informate che siano basate sul rischio.

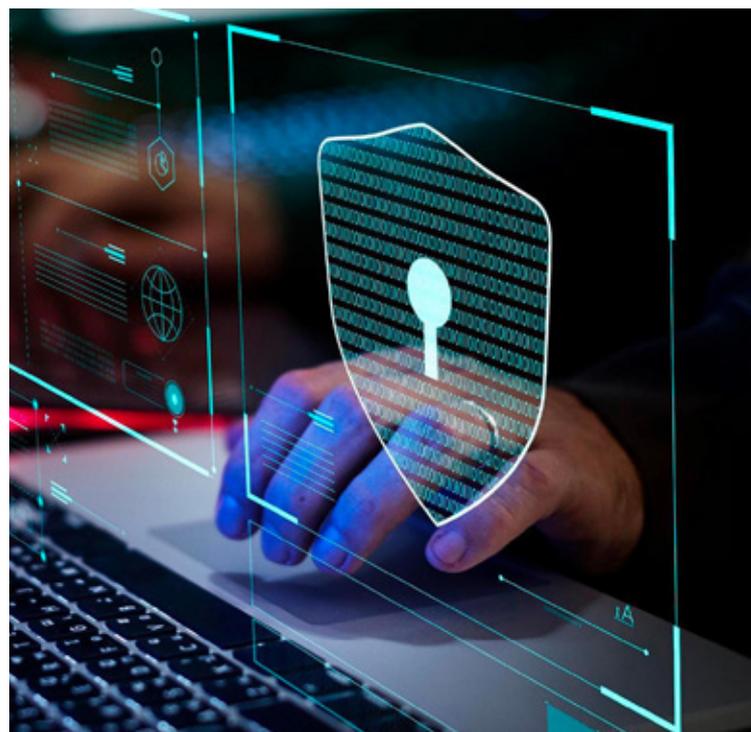
Enel ha inoltre creato il proprio **"Cyber Emergency Readiness Team"** (CERT), per gestire e rispondere in modo proattivo agli incidenti cyber, incentivando inoltre la collaborazione e lo scambio di informazioni all'interno di una rete di partner internazionali accreditati. Con il perfezionamento dell'accordo con il CERT nazionale USA, il numero di accreditamenti ha raggiunto quota 9: Romania, Italia, Cile, Argentina, Perù, Colombia, Brasile, Spagna e USA. Il CERT di Enel fa anche parte di Trusted Introducer, un servizio che comprende 464 CERT distribuiti in 72 Paesi. A settembre 2018 ha aderito anche a FIRST (Forum of Incident Response and Security Teams), la più grande ed estesa comunità del settore con 602 membri dislocati in 99 Paesi. Nel corso del 2022, inoltre, il modello operativo del CERT è stato potenziato con la creazione di un team interno di analisti di sicurezza. Il nuovo modello operativo ha superato quello precedente, implementando l'internalizzazione delle attivi-

tà di monitoraggio e gestione degli incidenti e potenziando, quindi, le attività h24.

Definizione della strategia di sicurezza informatica

La strategia di cyber security ingloba le attività legate alla definizione di obiettivi e priorità, al fine di indirizzare e coordinare le iniziative di investimento per il Gruppo nel suo complesso e garantire l'aderenza alle policy di cyber security, la definizione di target, il reporting manageriale e il monitoraggio continuo delle attività di sicurezza in corso. Tale processo è guidato dal CISO e fa leva su una stretta integrazione e sinergia con le diverse aree di business, che comunicano le proprie esigenze, analizzano le opportunità, gestiscono eventuali criticità e propongono possibili iniziative.

In particolare, la definizione della strategia è un'attività iterativa, basata sulla condivisione e sul consolidamento del target di "risk posture" del Gruppo. I diversi attori coinvolti analizzano le varie opzioni e le possibili iniziative all'interno della rispettiva area di business per valutarne la fattibilità, garantire il consenso e il relativo finanziamento. L'unità di Cyber Security guida il processo e, insieme agli altri attori rilevanti, consolida progressivamente, in un documento di proposta di cyber security strategy, aspetti come lo scenario futuro, gli obiettivi e le possibili iniziative strategiche, con una stima del budget di alto livello e la definizione delle priorità.



Cyber security incident management

La molteplicità e la complessità degli ambienti in cui operiamo (dati, industry e persone) e delle componenti tecnologiche (per esempio, sistemi business-critical come SCADA – Supervisory Control and Data Acquisition, smart grid e contatori elettronici), sempre più integrati nella vita digitale del Gruppo, hanno reso necessaria la definizione di un sistema strutturato di cyber security. Da qui, il modello di cyber defense basato su una visione sistemica che integra il settore IT (a partire dal cloud fino al data center e al cellulare), l'OT (tutto ciò che riguarda il settore industriale, come il telecontrollo degli impianti) e l'IoT (l'estensione della comunicazione e dell'intelligenza artificiale al mondo degli oggetti).

Il CERT, attraverso i sistemi di monitoraggio, raccoglie ogni giorno 3 miliardi di eventi relativi agli asset aziendali da 7mila data source, li mette in correlazione sfruttando l'analisi automatica, e produce in media un centinaio di "incident". Gli incidenti sono classificati secondo una specifica matrice di impatto (Enel Cyber Impact Matrix), su una scala da 0 a 4, avvalendosi delle migliori capacità di correlazione degli eventi derivanti dall'adozione di servizi all'avanguardia.

La stragrande maggioranza degli incidenti è classificata al **livello 0/1**, non ha un impatto significativo sui sistemi del Gruppo ed è automaticamente o semi-automaticamente bloccata e/o gestita dalle difese aziendali in essere, che in questo modo prevencono e/o riducono l'impatto di potenziali attacchi cyber.

Gli incidenti classificati al **livello 2/3/4** hanno un impatto potenziale sul Gruppo e sono gestiti dagli analisti del CERT coinvolgendo gli stakeholder interessati. Grazie ai servizi di protezione, ogni giorno, nel 2022 **il CERT ha bloccato in media 1,2 milioni di e-mail a rischio, 57 virus, 172 attacchi a portali web e 1,3 milioni di connessioni a siti pericolosi.**

Nel corso del 2022 il CERT di Enel ha risposto a: **175 incidenti di sicurezza informatica con livello di impatto 2; 16 incidenti con livello di impatto 3; 0 incidenti con il più alto livello di impatto, il 4.**

Nei casi rilevati, al fine di consentire una risposta efficiente e rapida, così da minimizzare gli impatti su persone, servizi e asset, sono state attivate tutte le procedure definite per la relativa gestione.

In particolare, quando un incidente di cyber security si traduce in una potenziale violazione dei dati, vengono immediatamente intraprese le azioni necessarie, in linea con la policy del Gruppo Enel "**Personal Data Breach Management**". Nell'eventualità che possa generarsi una situazione di crisi che metta a rischio la business continuity aziendale, gli asset, la reputazione e/o la redditività del Gruppo Enel, le opportune azioni sono intraprese immediatamente, in linea con la specifica policy di Gruppo in materia di "Gestione degli eventi critici".

La policy "**IT Service Continuity Management**", inoltre, formalizza un processo avente l'obiettivo di ridurre a un livello accettabile il rischio che impatta sulla disponibilità dell'infrastruttura IT, di supportare le esigenze di business continuity, e di garantire il ripristino dei servizi IT in base ai risultati derivanti da una Business Impact Analysis, nel momento in cui si dovesse verificare una grave interruzione, anche causata da un incidente.

La tecnologia di EDR (Endpoint Detection and Response) è volta al blocco delle violazioni attraverso l'uso di feature innovative e paradigmi avanzati, in grado non solo di identificare i virus e i malware presenti sugli endpoint, ma anche di rilevare sequenze sospette di eventi tecnici che potrebbero rivelarsi parte di un tentativo di attacco.

Relativamente al numero degli eventi di sicurezza informatica registrati nel corso del 2022, di seguito si riportano i dettagli.

	2022
Numero totale di violazioni della sicurezza delle informazioni o altri incidenti di sicurezza informatica ⁽¹⁾	0
Importo totale delle multe/sanzioni pagate in relazione a violazioni della sicurezza delle informazioni o altri incidenti di sicurezza informatica	0
Numero totale di clienti e dipendenti impattati da data breach che hanno interessato il Gruppo	0
Numero totale di data breach ⁽²⁾	0

(1) Il valore riferito alla numerosità del KPI "Numero totale di violazioni della sicurezza delle informazioni o altri incidenti di sicurezza informatica" è relativo agli incidenti di livello 4.

(2) Il KPI "Numero totale di data breach" si riferisce al numero di eventi occorsi per effetto di un incidente di sicurezza informatica (ciò implica che la numerosità riportata non contempla eventuali disclosure occorse per effetto di incidenti non digitali).

Inoltre, al fine di rafforzare la capacità di prevenzione, reazione, e gestione degli incidenti, con il coinvolgimento del personale attivo negli ambienti di produzione, sono stati eseguiti alcuni **cyber exercise**, esercitazioni volte alla simulazione di un reale attacco. Al termine di ciascuna esercitazione sono stati prodotti report contenenti le azioni di dettaglio circa lo

svolgimento della simulazione, con l'obiettivo di valutare, in un'ottica di continuo miglioramento, qualità e completezza del materiale fornito a supporto delle decisioni, tempi di esecuzione per ogni fase e coerenza con le procedure. Nel 2022, in particolare, sono stati eseguiti 50 cyber exercise in ambienti industriali in 11 Paesi di presenza del Gruppo.

Principali progetti e iniziative

Tutti i progetti, i programmi e le iniziative di cyber security mirano a evitare, mitigare o porre rimedio ai rischi di sicurezza informatica per l'intero Gruppo. Di conseguenza,

tutte le attività, gestite con un approccio risk-based e secondo il principio di security by design, generano un processo di due diligence continuo che include anche attività di self assurance.

CERT – RISK MONITORING EXTENSION

“**CERT – Risk Monitoring extension**”. Il CERT impiega tecnologie emergenti come SOAR (Security Orchestration, Automation and Response) e machine learning a supporto dei Big Data, che consentono di automatizzare e velocizzare le attività di gestione degli incidenti e di sfruttare una migliore visibilità sulle minacce informatiche, aumentando l'efficienza nella gestione di quelle nuove e delle relative indagini. In particolare, grazie al sistema SOAR, attraverso la definizione di flussi operativi, è possibile automatizzare task ripetitivi; mentre attraverso il machine learning, una

branca dell'intelligenza artificiale, è possibile apprendere o migliorare le capacità di rilevamento sulla base dei dati disponibili.

Queste tecnologie consentono di accelerare, arricchire e tracciare in modo consistente le attività necessarie durante le fasi di analisi e gestione di un incidente, fornendo un grande supporto all'analista che può così parallelizzare e concentrarsi sui compiti più complessi che richiedono l'intervento umano.

MULTI-FACTOR AUTHENTICATION (MFA)

“**Multi-Factor Authentication (MFA)**” è una soluzione cloud utilizzata per imporre il metodo di identificazione per gli utenti durante la procedura di autenticazione. L'adozione della MFA permette di riconoscere una persona che accede a un sistema tramite un secondo fattore di autenticazione, fruibile tramite SMS o app installata sullo smartphone. La soluzione MFA è in linea con il quadro re-

golatorio ed è fortemente raccomandata per contrastare le minacce emergenti di furto di credenziali, anche basate su tecniche di social engineering (per esempio, il phishing o eventuali comportamenti degli utenti non aderenti alle policy). L'adozione della soluzione è a regime per tutti gli utenti.

CONTROLLI DI ASSURANCE

Controlli di assurance (Ethical Hacking, Vulnerability Assessment). Tali attività vengono svolte in maniera costante sia con l'ausilio di strumenti automatici sia manualmente, al fine di valutare e quantificare eventuali debolezze in ambienti IT, OT e IoT (applicazioni, sistemi, dispositivi IoT, ar-

chitetture e/o infrastrutture). Nel 2022 sono stati eseguiti 1.587 controlli. A valle degli stessi è possibile identificare le misure più idonee per eliminare o mitigare le vulnerabilità o le minacce rilevate e, di conseguenza, gli eventuali exploit dannosi associati.

DMARC “E-MAIL FRAUD DEFENSE”

DMARC “E-mail Fraud Defense”. La soluzione completa la mappa applicativa a copertura delle minacce di spam, phishing e dei tentativi di frode. Grazie a quest'ultima, tutti i domini di posta elettronica di Enel sono stati configurati

per consentire il blocco delle e-mail con un indirizzo mittente falso che sfrutta il brand di Gruppo. Il deployment è avvenuto sull'intero perimetro, fornendo così una copertura totale dei domini.

Collaborazioni con organismi ed enti esterni

In linea con l'approccio Open Power, consideriamo la rete di relazioni con le realtà esterne e le organizzazioni un elemento chiave nella strategia di cyber security, per condividere le migliori pratiche e i modelli operativi, sviluppare e rafforzare i canali di condivisione delle informazioni e contribuire alla definizione di standard e normative. Nel corso del 2022 abbiamo fornito feedback in consultazioni pubbliche che hanno contribuito al disegno normativo in tema di cyber security, anche attraverso azioni di drafting legislativo, promuovendo l'armonizzazione dell'attuale panorama normativo in materia e l'attuazione di un approccio basato sul rischio e sul principio di security by design. Fra le collaborazioni avute, si annoverano quelle volte alla costruzione di assetti più omogenei nella definizione della tassonomia degli incidenti di sicurezza, di più organici criteri di classificazione degli stessi, unitamente a una modalità più armonica nelle procedure di notifica in contesti europei. Queste collaborazioni sono anche guidate da un composito panorama normativo in materia di cyber security, sia in termini di aumento delle norme prodotte sia in termini di complessità, principalmente dovuta alle nuove normative che si aggiungono ogni anno, oltre che all'eterogeneità dei requisiti e dei metodi di adozione.

In questo senso, il processo mirato alla compliance normativa può avere un forte impatto, sia sui processi aziendali sia sull'infrastruttura tecnologica, richiedendo un grande sforzo in termini di gestione e monitoraggio.

Inoltre, tenendo in considerazione il contesto di compliance normativa, **nel 2022 non sono state rilevate non-conformità a standard o regolamenti in tema di sicurezza informatica.**

Negli ultimi anni è stato definito e sviluppato un solido network, interagendo anche con stakeholder rilevanti del settore energetico quali ANEEL (Agência Nacional de Energia Elétrica) e ONS (Operador Nacional do Sistema Elétrico) in Brasile e CNO (Consejo Nacional de Operación) in Colombia. Abbiamo preso parte, per esempio, al team di Confindustria Digitale, che ha lo scopo di dare contributi allo sviluppo dell'ecosistema digitale italiano, abbiamo partecipato ai gruppi di lavoro del World Economic Forum, e contribuito negli ultimi anni alla pubblicazione di diversi rapporti tra cui "Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain" e "Cyber Resilience in the Electricity Industry: Analysis and Recommendations on Regulatory Practices for the Public and Private Sectors".

Inoltre, Enel X, Gridspertise ed Enel Grids hanno raggiunto

un importante traguardo nel campo della sicurezza delle informazioni, ottenendo la **certificazione ISO 27001**. Questo importante risultato certifica alcuni processi dotati di un sistema di gestione della sicurezza delle informazioni – politiche, procedure e linee guida per fornire ai clienti prodotti e servizi trusted.

Formazione e informazione

Il "Cyber Security Awareness Program" è diventato un'iniziativa costante e continuativa a livello di Gruppo, volta a diffondere la cultura della sicurezza informatica e aumentare la consapevolezza in merito alle minacce e agli attacchi che hanno come obiettivo il vettore umano. Tale programma contribuisce difatti alla digitalizzazione, poiché crea una cultura della sicurezza informatica, cambia il comportamento delle persone al fine di ridurre il rischio cyber, sviluppa competenze tecniche sulla sicurezza informatica e rende le persone la prima linea di difesa aziendale. Si avvale, inoltre, di diversi canali di comunicazione e strumenti di diffusione, comprendendo sia campagne di comunicazione sia iniziative di formazione dedicate per cluster di persone. Nello specifico, nel corso del 2022, sono stati realizzati 19 eventi di knowledge sharing a livello Globale su tematiche di cyber security e sono state eseguite diverse iniziative anche a livello locale. A titolo esemplificativo, nell'ambito di tali iniziative, la Policy no. 1097 "Rules of Behavior for Digital People", è stata integrata con una guida rapida, disponibile in tutte le principali lingue adottate dal Gruppo (5 differenti lingue), volta ad agevolare una veloce consultazione dei temi per indirizzare il corretto uso di risorse digitali. Sono stati inoltre predisposti e diffusi bollettini e notizie attraverso la intranet aziendale, e messi a disposizione documenti per mantenere un aggiornamento costante su tali temi. Tutto ciò è stato reso possibile anche grazie alla piattaforma di awareness "TheRedPill", la piattaforma di Gruppo attraverso cui sono stati erogati contenuti e moduli formativi volti a potenziare la cultura in ambito di sicurezza informatica, consentendo il miglioramento continuo delle iniziative di formazione e l'esecuzione di campagne di phishing simulato. L'obiettivo è generare e potenziare la consapevolezza sulle principali tematiche di cyber security, di indirizzare eventuali esigenze di upskilling e reskilling e di insegnare come difendersi da eventuali attacchi. Nel 2021, anno in cui ha avuto luogo l'aggiornamento della piattaforma, sono state lanciate quattro campagne globali di phishing simulato, un knowledge assessment e una campagna di sensibilizzazione. Nel 2022 sono state lanciate ulteriori iniziative a livello globale, quali la diffusione del modulo "Antiphishing Kit", o il lancio del

“People Cyber Empowerment Journey”, ovvero il programma che mira a portare le persone di Enel a essere la prima linea di difesa informatica. Inoltre, sono state disegnate e lanciate 6 campagne di phishing simulato, 3 campagne di sensibilizzazione relative alla protezione dell'identità digitale, alla protezione dei dati e dei device, e 19 eventi volti alla diffusione della cultura di sicurezza informatica (c.d. “knowledge sharing”).

In aggiunta alle iniziative di diffusione e comunicazione, nel corso del 2022 sono proseguite le campagne di phishing simulato rivolte all'intera popolazione Enel, con l'obiettivo di allenare i dipendenti a riconoscere le e-mail malevole. A seguito dei risultati ottenuti dalle campagne di phishing, sono state realizzate iniziative specifiche per aumentare la

sensibilità e la consapevolezza dei dipendenti (per esempio, specifiche infografiche, istruzioni e linee guida sono state condivise con coloro i quali non sono stati in grado di riconoscere l'e-mail di phishing).

Il progetto **Open Tech Journey** è proseguito con l'obiettivo di rendere disponibili corsi di formazione incentrati su temi tecnologici, promuovendo le capacità interne per diffondere la conoscenza su temi strategici e per gestire esigenze di upskilling e reskilling. In tale ambito è stata attivata la **Cyber School**, con un'offerta di sette corsi sui principali temi legati alla cyber security. Tutti i corsi sono stati ingegnerizzati e resi disponibili a tutta la popolazione Enel in modalità e-learning, con l'obiettivo di raggiungere competenze multi-specialistiche nelle diverse realtà aziendali del Gruppo.

