Executive Summary

La sicurezza dei dati immagazzinati e comunicati tramite le infrastrutture informatiche è da tempo un tema di grande attualità, sia dal punto di vista della privacy, sia da quella della protezione dei dati «mission critical».

In un mondo sempre più interconnesso, le minacce provengono dalle fonti più disparate (e più remote), e gli autori degli attacchi sono sempre più difficili da individuare. Si parla in questo senso di **cyberspazio** e di **cybersecurity.**

La cybersecurity può quindi essere intesa come:

L'insieme di **strumenti, procedure e sistemi** che consente a una entità (ad esempio, una nazione, una organizzazione, un cittadino)...

...la protezione dei propri asset fisici e della **confidenzialità, integrità e disponibilità delle proprie informazioni** attraverso un'attività di **prevenzione, rilevazione e risposta** agli attacchi provenienti **dal «cyberspazio»**

Il concetto di cybersecurity, pertanto, tende a includere gli ambiti tipici dell'**ICT security** (ovvero la protezione dei dati – sia all'interno dei database che nell'ambito dei flussi di comunicazione sulle reti informatiche), ma include anche la protezione degli **asset fisici**.

Gli attacchi provenienti dal cyberspazio che un'impresa si trova a dover fronteggiare sono tipicamente perpetrati da **soggetti** molto diversi:

- Hacker «isolati»

- Organizzazioni terroristiche
- Nazioni
- Concorrenti
- Business partners (fornitori di prodotti/servizi)
- Dipendenti

Va precisato che in taluni casi questi soggetti rappresentano i **«mandanti»** dell'operazione, mentre in altri si tratta di **esecutori**. Va inoltre sottolineato che alcuni di tali soggetti possono essere dei «veicoli» involontari (una sorta di «portatori sani di infezione»). E' il caso tipicamente dei dipendenti e di alcuni business partners (consulenti IT, revisori contabili, ecc), i quali hanno maggiore probabilità di accedere ai sistemi informativi aziendali (e di connettersi alle reti LAN) e possono contribuire ad «aggirare» le difese perimetrali e contribuire al successo di un attacco, qualora non rispettino le policy e le precauzioni dovute nell'espletamento delle loro attività (es: credenziali condivise, PC/USB pen infette, ecc).

Anche le finalità di un attacco possono essere molteplici. Tipicamente sono riconducibili a tre macro-obiettivi, illustrati nella figura a pagina seguente.

Perché uno studio sul settore energetico?

Il settore dell'energia (e in particolare la filiera elettrica) è caratterizzato da trend innovativi che ne stanno aumentando la possibile esposizione ad attacchi cibernetici. Si fa riferimento in particolare:

- al crescente peso del peso delle **fonti rinnovabili**
- alla diffusione del modello **«prosumer»**
- all'impatto della **digitalizzazione** (cioè del crescente uso di tecnologie ICT per gestire tutte le attività della

AMBITO	DESCRIZIONE	FINALITA'/ DETERMINANTI
CYBER CRIME	**Atti criminali** commessi **usando sistemi informativi o reti di comunicazione elettroniche** al fine di perseguire vantaggi di tipo economico	Economiche
CYBER TERRORISM	**Attacchi** che, attraverso l'utilizzo e lo sfruttamento di computer o reti di comunicazione, sono **volti** a generare incidenti tali da **generare paura o danni** nei soggetti «target»	Ideologiche
CYBER WARFARE	**Attacchi**, che sfruttando computer o le reti di comunicazione, sono **volti a danneggiare gli asset fisici o digitali di una nazione al fine di comprometterne l'operatività**	Politiche/ Militari

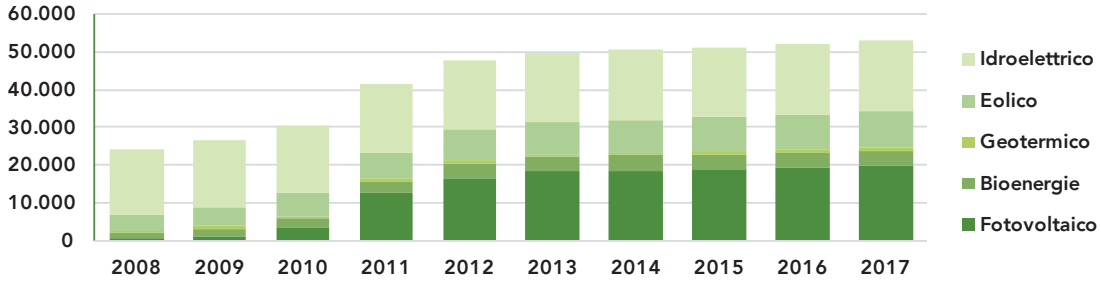
catena del valore dei vari operatori della filiera - la cosiddetta «digital energy»).

Come si può notare, i primi due trend sono peculiari della fase di produzione dell'energia elettrica, mentre la digitalizzazione ha un impatto sicuramente più pervasivo all'interno della filiera, anche se vi sono ovviamente dei legami tra i vari trend (es: la generazione distribuita è resa possibile dalle tecnologie di gestione «intelligente» della rete).

In particolare, la potenza installata da **fonti rinnovabili** ha raggiunto nel 2017 i **53 GW**, contribuendo a coprire il **36,2%** della produzione annua (pari 103,4 TWh). In base alle previsioni contenute nel documento che illustra la **Strategia Elettrica Nazionale**, tale percentuale dovrebbe salire al **60%** entro il 2030 (per un valore pari a 184 TWh).

La diffusione degli impianti di produzione da fonti rinnovabili comporta un vertiginoso **incremento del numero di impianti** di generazione (parchi fotovoltatici, eolici, ecc), cui corrisponde anche un significativo numero di **nuovi entranti** nel settore (tipicamente con scarsa esperienza e ridotta conoscenza dei rischi di natura «cyber»).

Similmente, la nascita dei **«prosumer»** (ovvero di imprese industriali, attività commerciali, famiglie che ricoprono il duplice ruolo di generatori e consumatori di energia) aumenta in modo esponenziale **il nu-**



mero di attori connessi alla rete in qualità di produttori (sebbene di piccola/piccolissima taglia). Aumenta di conseguenza la cosiddetta **«superficie d'attacco»**, cioè la probabilità che attacchi (soprattutto se di tipo «phishing») vadano a buon fine.

La **digitalizzazione** della filiera (la cosiddetta «digital energy») coinvolge invece tutti gli attori della filiera, e costituisce tipicamente un abilitatore di nuove funzionalità e di nuovi servizi per i vari attori operanti all'interno della filiera elettrica. Tra gli effetti più significativi è possibile annoverare:

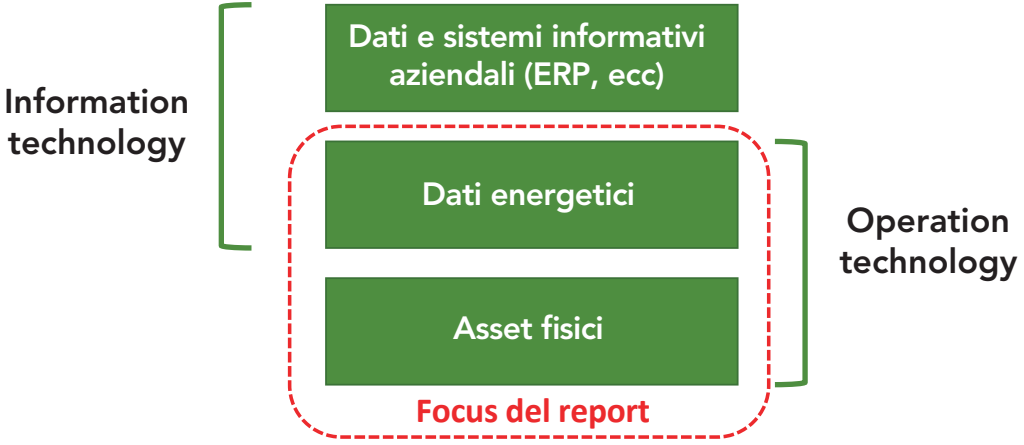
- lo sviluppo delle **«smart grid»**, ovvero delle reti «intelligenti» (fondamentali peraltro nel passaggio al modello di generazione distribuita tipico delle rinnovabili)
- nella fase di **generazione**, la possibilità di introdurre strumenti di **stima della produzione** di energia (particolarmente importanti nel caso degli impianti a fonte rinnovabile), di ottimizzazione delle attività di produzione (grazie a funzionalità di telemonitoraggio e telecontrollo) e di **predictive maintenance**
- per gli end-user, la possibilità di contenere i consumi di energia (sugli impianti già installati), di ottimizzare gli investimenti in efficienza energetica, nonché di utilizzare i dati energetici per fare manutenzione preventiva

Tutte queste nuove potenzialità comportano una **crescente interconnessione** degli impianti (di produzione, trasmissione, distribuzione dell'energia, nonché degli utilizzatori finali), il che ovviamente espone tali asset alle stesse minacce cui sono soggetti i sistemi informativi e le reti aziendali.

Ne è una riprova il crescente numero

di attacchi perpetrati ai danni delle infrastrutture energetiche: tra questi, i più famosi sono sicuramente quello ad opera del **trojan Havex**, che ha infettato finora più di 2.000 apparati dotati di ICS tra Europa e USA, e quello che ha bloccato l'intera rete di distribuzione della compagnia ucraina **Kyivoblenergo** nel dicembre 2015.

Da qui la decisione di focalizzare questo report sul tema della **sicurezza industriale**, e quindi sui dati energetici e sugli asset fisici utilizzati nell'ambito delle operations, tralasciando le problematiche «classiche» dell'ICT security.



I rischi di natura «cyber» per la filiera elettrica

Il rischio legato alla crescente digitalizzazione delle operations è particolarmente elevato perché, dal momento che storicamente gli asset industriali lavoravano in modalità **«stand-alone»**, essi non erano soggetti ad attacchi di natura informatica. Di conseguenza, i sistemi operativi e i software installati per gestire tali asset **non venivano quasi mai aggiornati** (e quindi le vulnerabilità mai eliminate). Da qui la necessità di prevedere opportune soluzioni di tipo tecnologico e organizzativo, volte a minimizzare il rischio di incidenti di sicurezza nel momento in cui tali dispositivi vengono interconnessi in rete, o comunque, iniziano a scambiare dati con altri dispositivi hardware (come una banale chiavetta USB).

A questo problema, che riguarda tutto il «parco installato», si aggiunge quello relativo agli investimenti in nuovi asset, che devono adeguarsi al nuovo contesto e garantire quindi adeguati **standard minimi di sicurezza.**

Nel corso dello studio sono stati in primo luogo analizzati i rischi per i diversi stadi della filiera elettrica, e precisamente:

- **Player della generazione**, i quali possiedono e gestiscono gli impianti di produzione
- **Trasmission System Operator** e **Distribution System Operator**, chiamati a gestire rispettivamente la rete di trasmissione e quella di distribuzione
- **Prosumer**: una figura intermedia che è contemporaneamente consumatore e produttore di energia, ed è quindi esposta ai rischi che caratterizzano entrambe le categorie.

- **Consumatori di energia** (di natura industriale o residenziale)

Considerato il focus dell'analisi, in questo studio non sono stati considerati i puri retailer di energia.

Per ciascuno stadio si è proceduto ad analizzare:
- I possibili **impatti sulle attività (e sugli asset)** degli attacchi di natura cyber
- I conseguenti **danni economici**

In generale, gli attacchi di natura cyber in ambito OT sono mirati a:
- Catturare **informazioni** sui parametri di funzionamento di apparati e sistemi
- **Alterare** il funzionamento di apparati e sistemi, interrompendo flussi di dati o alterando i dati di input (per esempio attraverso i sistemi di telecontrollo), fino a giungere al danneggiamento degli asset .

A titolo d'esempio, nella figura seguente sono riportati i possibili rischi operativi e i conseguenti impatti economici nel caso dei player della generazione (e dei prosumer, nella veste di produttori di energia elettrica).

Dopo aver analizzato le possibili conseguenze per i singoli attori della filiera, l'attenzione si è spostata sul rischio «di sistema», ovvero sulla possibilità che attacchi di natura cibernetica possano mettere in crisi la stabilità della rete elettrica nazionale, o comunque comportino degli extra-costi significativi per il ribilanciamento tra domanda e offerta (è noto, infatti, che la rete elettrica deve essere caratterizzata sempre un bilanciamento - quasi in tempo reale - tra domanda e offerta di energia).

In particolare, gli approfondimenti

	RISCHI	IMPATTI ECONOMICI
PLAYER GENERAZIONE «PURA»	• **Mancata produzione di energia elettrica** • **Inaccessibilità ai sistemi di monitoraggio e telecontrollo** (perdita di visione e controllo sugli impianti) • **Danni fisici agli impianti di produzione**	• **Riduzione del margine di contribuzione** (legato alla mancata vendita d'energia) • **Penali da mancata vendita energia elettrica** • **Mancato margine da fornitura di servizi ancillari** • **Costi legati ai danni a impianti o persone**
PROSUMER (NELLA VESTE DI PRODUTTORI)	• **Mancata produzione di energia elettrica** • **Danni agli impianti di produzione**	• **Riduzione dell'autoconsumo,** con conseguente **aumento della bolletta energetica** • **Marginalità legata alla mancata vendita d'energia** • **Costi legati a danni a impianti o persone**

hanno riguardato:

- L'analisi degli extra-costi per il sistema derivanti dalla diminuzione dell'energia prodotta nel corso di un anno da impianti a fonte rinnovabile (parchi fotovoltaici e eolici) a causa

di attacchi ripetuti e «distribuiti», tali da compromettere temporaneamente il funzionamento di tali impianti (in termini di ore di funzionamento e/o quantità di energia prodotta), con conseguente necessità da parte di Terna di ribilanciare la rete facendo ricorso al Mercato dei Servizi di Dispacciamento;
- L'analisi del potenziale rischio di black-out derivante dall'improvviso mancato apporto di energia da parte di un certo numero di impianti a fonte rinnovabile (a seguito di un incidente di natura «cyber» che porta al blocco temporaneo dell'operatività di tali impianti) in un momento di picco di domanda (quindi tipicamente in un giorno feriale estivo, caratterizzato da alte temperature, nelle ore di punta.

In particolare, i risultati delle simulazioni evidenziano che:
- Gli extra-costi generati dal ricorso più frequente al MSD appaiono tutto sommato abbastanza contenuti nei vari scenari ipotizzati (per esempio: nel caso di attacchi che portano a una riduzione del 50% della potenza erogata per il 10% delle ore medie annue di funzionamento, tali costi variano da circa 10 a oltre 80 mil€ a seconda dell'area geografica di riferimento, per un totale a livello italiano di circa 264 mil€)
- Assumendo come giorno di riferimento le ore 12 del 21 Luglio 2017 (uno dei giorni di picco massimo di domanda di energia nel corso del 2017), una riduzione improvvisa della potenza pari a 3 GW (soglia oltre la quale si ritiene più probabile il rischio di instabilità e di conseguente black-out temporaneo della rete) si sarebbe

raggiunta con un'indisponibilità contemporanea del 12,7% della potenza generata dagli impianti eolici e fotovoltaici. Una percentuale piuttosto significativa, quindi, anche se va tenuto presente che la percentuale di energia fornita da fonti rinnovabili è destinata ad aumentare nel futuro, per cui l'incremento della «superficie d'attacco» potrebbe incrementare i rischi di instabilità del sistema, qualora non si investa sufficientemente nella sicurezza di tali impianti, nonché in soluzioni finalizzate a garantire comunque la stabilità della rete.

Il quadro normativo di riferimento

Data il ruolo strategico ricoperto dalla rete elettrica all'interno di qualsiasi nazione, è naturale che la sicurezza di tali infrastrutture rappresenta da sempre una priorità per chi è chiamato a governarle.
La crescente esposizione ai rischi di natura informatica cui vanno incontro le infrastrutture critiche ha portato all'emanazione di direttive (a livello internazionale e nazionale) e a iniziative finalizzate a garantire un'adeguata protezione e una risposta adeguata in caso di crisi cibernetiche a livello nazionale.

Tra queste risultano particolarmente rilevanti nel contesto italiano:

- **la direttiva UE «NIS»** (Network and Information Security – EU 2016/1148)
- **il Quadro Strategico Nazionale Per La Sicurezza Dello Spazio Cibernetico**
- **il DPCM 13 aprile 2017** (noto come DPCM «**Gentiloni**»)
- **il Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica**

In particolare, la **direttiva NIS** (recentemente recepita in Italia con DPCM del 16 maggio 2017 e in vigore dal 26 giugno scorso) prevede che all'interno di ciascun Stato membro vengano individuati i cosiddetti «operatori di servizi essenziali» all'interno di alcuni settori fondamentali (tra cui quello energetico).

Tali operatori saranno quindi obbligati a:

- **adottare misure adeguate** atte a prevenire e minimizzare l'impatto di **incidenti a carico della sicurezza della rete** e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali
- **fornire** all'autorità competente NIS:
  - le **informazioni necessarie a valutare la sicurezza della loro rete** e dei sistemi informativi, compresi i documenti relativi alle politiche di sicurezza
  - la **prova dell'effettiva attuazione delle politiche di sicurezza**, come i risultati di un audit sulla sicurezza svolto dall'autorità competente NIS o da un revisore abilitato
- **notificare** al Computer Security Incident Response Team **(CSIRT)** nazionale (e per conoscenza alle autorità competenti NIS) **ogni incidente** avente un **impatto rilevante** sulla continuità del servizio fornito.

In ossequio a quanto richiesto dall'Articolo 7 della Direttiva, il decreto di recepimento prevede inoltre l'adozione di una **strategia nazionale di sicurezza cibernetica** da parte del Presidente del Consiglio dei Ministri

Tale strategia dovrà prevedere in particolare le misure di **preparazione, risposta e recupero** dei servizi a seguito di incidenti informatici, la definizione di un **piano di valutazione dei rischi informatici e programmi di formazione e sensibilizzazione** in materia di sicurezza informatica.

Gran parte degli elementi costituenti tale strategia sono peraltro già contenuti (a grande linee) nei documenti programmatici già emanati a livello nazionale, ovvero nel **Quadro strategico nazionale per la sicurezza dello spazio cibernetico** del 2013 e nel successivo **Piano nazionale per la protezione cibernetica e la sicurezza informatica** del 2017.

In questo ambito va infine segnalato che la **Strategia Energetica Nazionale** prescrive due differenti linee di azione con riferimento alla cybersecurity, riguardanti rispettivamente:

- Lo sviluppo di **un piano di ricerca nel settore elettrico** (che include attività di modellazione, simulazione e di natura sperimentale, nonché la partecipazione a tavoli di lavoro per la definizione di standard e la certificazione)
- Lo sviluppo delle **collaborazioni a livello internazionale** (per esempio con NATO ed ENISA) e il rafforzamento delle attività di **cooperazione pubblico-privato a livello nazionale.**

Dall'esame del framework regolatorio si nota come, fatta eccezione per le iniziative previste nell'ambito della SEN, le direttive non facciano riferimento specifico al settore elettrico. Questo comporta una certa «generi-

cità» delle misure prescritte, che lascia ampi margini di interpretazione e potrebbe rendere piuttosto «complicato» l'adeguamento alle norme (e quindi le attività di compliance).

Sorprende, inoltre, che tra gli operatori di servizi essenziali del settore energetico non figurino i produttori di energia.

Le soluzioni per una corretta gestione della security e il ruolo degli standard

Per rispondere alle minacce di natura «cyber», gli operatori della filiera elettrica sono chiamati a rispondere mettendo a punto un **cybersecurity management system** in ambito industriale (in modo del tutto analogo a quanto avviene per l'IT «tradizionale»), tenendo conto delle peculiarità dell'ambiente OT (per esempio, la priorità del requisito di disponibilità rispetto all'integrità e alla riservatezza).

Si tratta di un insieme di processi, risorse e adeguati meccanismi di governance che consentano a un'impresa di garantire un adeguato livello di sicurezza (quindi un'esposizione al rischio in linea con le normative di riferimento e/o i valori target fissati). Le attività previste comprendono:

- Le risk analysis
- L'identificazione delle contromisure adeguate
- Monitoraggio e miglioramento continuo
- Sensibilizzazione e formazione
- La definizione di policy e guidelines.

Nella progettazione di tale sistema di gestione della cybersecurity (e in particolare nella definizione del

«cosa» proteggere e del «come» garantire un adeguato livello di sicurezza) un ruolo importante è ricoperto dagli standard.

In questo report abbiamo focalizzato l'attenzione sugli standard più rilevanti nell'ambito della sicurezza OT delle reti elettriche, e precisamente:

- ISA 62443
- IEC 62351
- NERC 1300 CIP
- NIST Cybersecurity Framework (e NIST 800-82)
- ISO 27019

Alcuni di tali standard sono caratterizzati da uno «scope» più ampio, e cercano di fornire delle guidelines per la progettazione dei sistemi di gestione della cybersecurity. Tra questi rientra sicuramente il **Cybersecurity Framework** sviluppato dal **National Institute of Standards and Technology (NIST)**. L'approccio sviluppato dal NIST consente di confrontare l'assetto di governance della cybersecurity con i modelli proposti e di identificare gli eventuali gap.

Anche l'ISO 27019 (che deriva dalla ISO27001 e ISO27002) è caratterizzato da un ambito di impatto piuttosto ampio. Esso infatti definisce **un insieme di regole/practice finalizzato a garantire la sicurezza dei sistemi di controllo e delle tecnologie di automazione** utilizzati nell'ambito della produzione, trasmissione/distribuzione dell'elettricità, del gas, del petrolio e del calore.

Lo **standard NERC CIP 1300**, messo a punto dalla North American Electric Reliability Corporation (NERC), identifica i requisiti minimi da implementare e mantenere al fine di garantire la sicurezza cibernetica degli asset presenti all'interno

dei sistemi generazione, trasmissione e distribuzione del sistema elettrico.

Lo **standard IEC-62443**, precedentemente noto con il nome di ISA 99, è stato sviluppato dall'International Society for Automation (ISA) e dall'International Electrotechnical Commission (IEC) nel 2010. Lo standard definisce **le linee guida** da utilizzare per incrementare la sicurezza informatica degli **Industrial Control System**. Lo standard definisce dei livelli «target» di sicurezza degli ICS. Questo ha delle ripercussioni importanti sui **produttori** degli apparati ICS, **in quanto**:

- Gli utilizzatori possono utilizzare questo standard per definire i requisiti di sicurezza nell'ambito delle gare o delle procedure di acquisto
- I vendor, di contro, possono «garantire» i livelli di sicurezza offerti dai propri prodotti ricorrendo a opportuna **certificazione**.

Anche lo standard **NIST 800-82** si focalizza sulla sicurezza dei sistemi ICS, attraverso una «defense-in-depth» strategy che prevede l'adozione di una serie di contromisure di varia natura (restrizione degli accessi, procedure di business continuity e disaster ricovery), nonché soluzioni organizzative ad hoc.

Infine, lo standard **IEC-62351** (*Power systems management and associated information exchange – Data and communications security*) è stato sviluppato dalla commissione tecnica 57 (TC 57) dell'International Electrotechnical Commission (IEC), e si focalizza sugli standard di sicurezza dei **protocolli di comunicazione** dei sistemi di generazione.

L'analisi condotta porta a conclude-

re che il livello di «copertura» degli standard sia oramai abbastanza avanzato, sia con riferimento al «*cosa proteggere*», che con riferimento al «*come*», anche se su quest'ultimo fronte ci sono ancora diversi sviluppi in corso (anche per via della continua evoluzione delle tecnologie – e delle vulnerabilità –).

La sfida adesso sembra consistere nel livello di adozione di tali standard, sia da parte delle imprese energetiche, sia da parte dei costruttori. In particolare, appare abbastanza cruciale il ruolo delle (grandi) imprese clienti nell' «imporre» l'adozione degli standard da parte dei loro fornitori, dal momento che quest'ultimi appaiono talvolta un po' riluttanti per via del timore di perdere il potere contrattuale derivante dal fatto di proporre soluzioni proprietarie.

L'indagine empirica: il punto di vista degli end-user

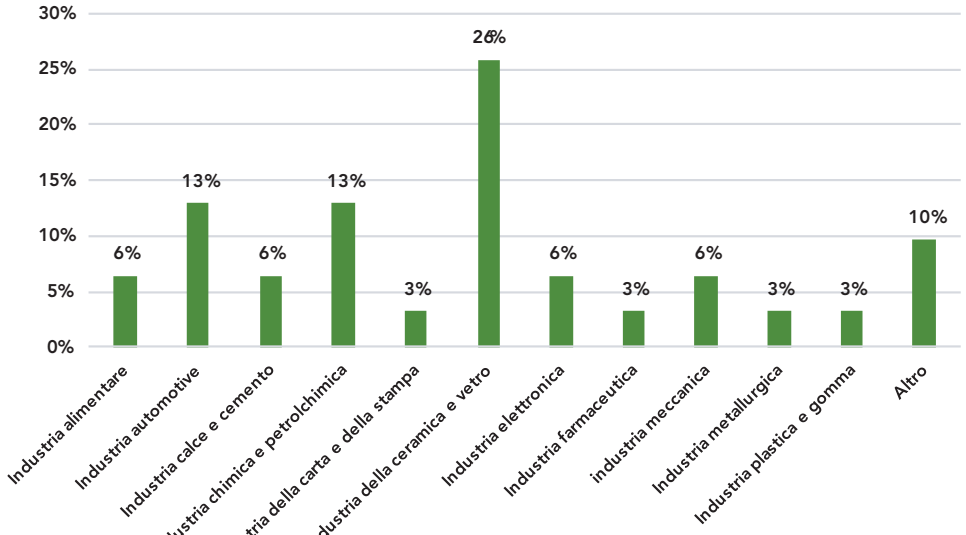
L'ultima parte del report si è focalizzata sugli end-user di natura industriale, con il duplice obiettivo di:

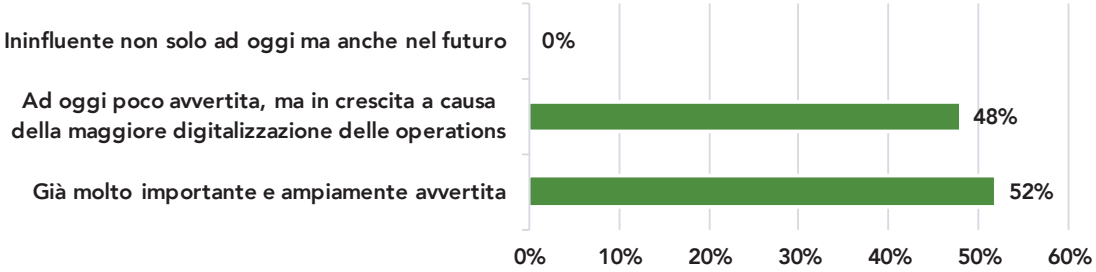
- verificare il grado di diffusione della **cultura della cybersecurity** in ambito **OT** all'interno del sistema industriale del nostro Paese, con particolare riferimento alle nuove minacce derivanti dalla digitalizzazione dei processi industriali
- Verificare (nel caso dei «prosumer») il livello di **consapevolezza dei rischi** legati alle attività di **generazione di energia.**

A tal fine è stata somministrata una survey a un campione di circa 700 imprese di varia dimensione e operanti in diversi settori, ottenendo 93 risposte. La distribuzione dei ri-

spondenti per settore di attività è riportato nel grafico sottostante. Come si può notare, i settori maggiormente rappresentati sono quelli della **ceramica e del vetro** (il 26% delle imprese rispondenti), **l'automotive e la chimica e petrolchimica** (entrambe al 13%).

Le risposte delle imprese evidenziano come l'importanza del tema della sicurezza OT sia in crescita. Circa metà dei rispondenti ha infatti affermato che il tema è già molto sentito,

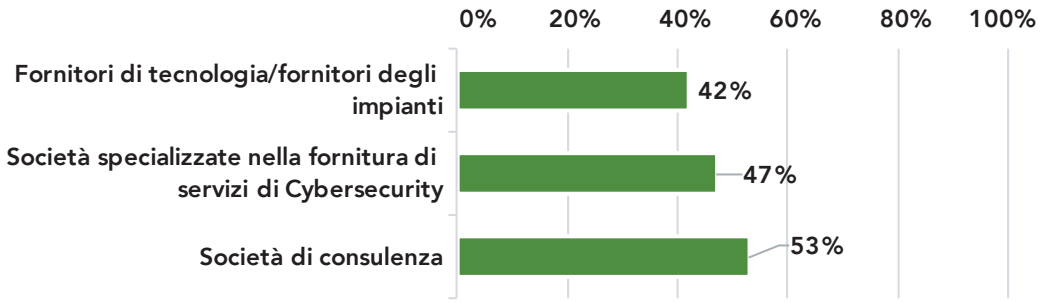




mentre la restante metà ritiene che l'attenzione crescerà notevolmente in futuro per via della crescente digitalizzazione.

Con riferimento agli aspetti organizzativi, la configurazione organizzativa più diffusa sembra essere quella «mista», che prevede l'utilizzo di risorse interne, supportate da terze parti (configurazione adottata dal **58%** delle imprese). Va altresì segnalato che il 10% dei rispondenti ha dichiarato di non aver ancora adottato nessuna soluzione organizzativa «stabile».

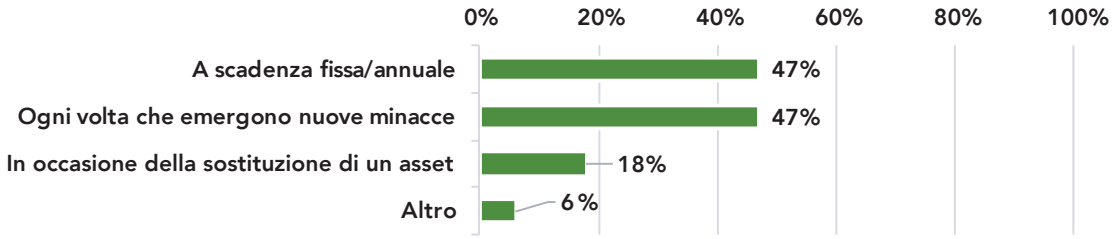
Analizzando più in profondità la natura dei business partner coinvolti nella gestione della cybersecurity OT, si scopre che le imprese si rivolgono sia a società di consulenza IT che a società specializzate nei servizi e soluzioni di cybersecurity. Da notarsi come solo il 42% dei rispondenti ha affermato di coinvolgere



i costruttori di apparati e impianti (nonostante la loro importanza strategica).

Questo risultato va visto in combinazione con le risposte ottenute in merito all'importanza attribuita dalle imprese alle **prestazioni di sicurezza degli apparati e dei componenti** nell'ambito del processo di aquisto. Solo il 10% dei rispondenti dichiara che tali performance sono rilevanti (e sono quindi inserite tra i requisiti), mentre poco più della metà delle imprese dichiara che tali prestazioni, per quanto prese in considerazione, non rappresentano un driver di scelta.

L'analisi del livello di strutturazione delle attività necessarie per una corretta gestione della cybersecurity fornisce dei risultati piuttosto preoccupanti: solo poco più di metà delle imprese, infatti, afferma di svolgere attività di **risk analysis** in ambito OT.



Ancora più preoccupante l'analisi delle **modalità** con cui viene volta tale attività. Come si può notare dal grafico sottostante, quasi la metà dei rispondenti afferma di condurla a cadenza fissa (tipicamente annuale), mentre un altro 47% dichiara di condurla quando emergono nuove minacce.

Ancor più significativo appare il dato sugli **investimenti**: solo il 23% delle imprese rispondenti ha infatti dichiarato di aver effettuato investimenti dedicati alla cybersecurity OT.

Nella parte finale della survey si è cercato di valutare la sensibilità delle imprese «**prosumer**» nei confronti dei rischi di natura cyber legati alla produzione di energia.

Più di metà dei rispondenti ha infatti dichiarato di essere anche produttore di energia: in particolare, il 45% ha installato **cogeneratori/trigene-**

ratori, mentre il 33% afferma di possedere un **impianto fotovoltaico**.

Risulta interessante osservare come le imprese prosumer ritengano questi impianti immuni a possibili attacchi di natura cyber. Infatti, solamente il **6% dei rispondenti** ritiene che l'operatività di questi impianti possa essere compromessa da attacchi cibernetici.

I risultati di questa indagine evidenziano come la cybersecurity OT sia considerata di fatto dalle imprese un tema strategicamente ancora poco rilevante (al di là delle dichiarazioni iniziali). La ridotta sensibilità sul tema e l'assenza di una casistica significativa di attacchi cibernetici volti a bloccare o a compromettere l'attività produttiva fa sì che le imprese preferiscano indirizzare gli investimenti verso altre aree.

Ancor più significative le risposte dei prosumer in merito ai rischi cui sono esposti gli impianti di produzione di energia da loro gestiti: il livello di consapevolezza risulta estremamente basso, tant'è che il problema non viene praticamente nemmeno preso in considerazione.

Paolo Maccarrone
Responsabile della Ricerca

Davide Perego
Project Manager