CYBERSECURITY, L'ELEFANTE NELLA STANZA DELLE UTILITY ITALIANE

Diego Pellegrino, portavoce di Arte (Associazione reseller e trader dell'energia) e Andrea Ferlin, ceo Professional Link

Sono cinque le tendenze sulle quali vediamo oggi concentrarsi i principali operatori del mercato dell'energia a livello globale: decarbonizzazione, efficienza energetica, liberalizzazione del mercato, utilizzo di nuove tecnologie e digital transformation.

L'implementazione degli ultimi due punti risulta particolarmente strategica anche per i primi tre, in una sorta di circolo virtuoso: l'industria dell'energia sta infatti studiando come utilizzare le nuove tecnologie per migliorare l'efficienza, la sostenibilità e la sicurezza delle infrastrutture.

L'adozione di intelligenza artificiale (IA) e machine learning (ML) è, per esempio, in grado di migliorare l'affidabilità delle infrastrutture energetiche riducendo il loro impatto ambientale grazie all'automatizzazione dei processi e alla manutenzione predittiva, che consentono di ridurre i tempi di fermo della produzione.

Parlare oggi di digital transformation nel settore energy significa dare per assodato l'utilizzo di tecnologie smart grid: le reti di informazioni e di distribuzione dell'energia elettrica. Queste sono sempre più diffuse anche nel nostro Paese poiché consentono una maggiore efficienza gestendo attivamente domanda e offerta di energia e monitorando i consumi in tempo reale; sono inoltre in grado di identificare e risolvere rapidamente i problemi, migliorando la sicurezza dell'approvvigionamento energetico e la resilienza dell'intera rete.

Smart grid, insieme ad intelligenza artificiale, machine learning, blockchain e Internet of things, promuovono la transizione verso un'economia a basso tenore di carbonio, oltre a permettere agli utenti di gestire i consumi in modo consapevole attraverso il monitoraggio e la programmazione degli elettrodomestici.

Un grande assente

Vediamo che decarbonizzazione, efficienza energetica, adozione di nuove soluzioni tecnologiche e liberalizzazione sono tendenze comuni alla maggior parte delle piccole e medie imprese italiane.

Tra le priorità del settore energy constatiamo, invece, non essere ancora considerata la sicurezza informatica.

L'atteggiamento delle utility italiane nei confronti della sicurezza informatica, soprattutto delle Pmi, è spesso caratterizzato da una certa inerzia, una riluttanza a investire in prevenzione e misure di sicurezza per proteggere le proprie infrastrutture e le attività da eventuali attacchi che, prima o poi, si verificheranno. Questo atteggiamento è dovuto alla mancanza di una cultura della cybersecurity (problema piuttosto diffuso nel nostro Paese) e alla scarsa consapevolezza dei rischi informatici, che si somma alla difficoltà di integrare nuove soluzioni tecnologiche all'interno dei sistemi di controllo delle infrastrutture preesistenti.

Tutto ciò porta spesso a non considerare la sicurezza informatica come strategica, un po' come la questione "elefante nella stanza": vale a dire un tema sostanziale ma sottovalutato, nella convinzione che i sistemi di sicurezza esistenti siano sufficienti per proteggere l'azienda.

Inoltre, l'aumento dei dispositivi connessi alla rete e le tecnologie IoT allargano ulteriormente la superficie di attacco dei criminali informatici, mettendo a rischio tramite un attacco alla singola utility anche privati cittadini e istituzioni su larga scala.

Ignorare "l'elefante nella stanza": i rischi della mancata adozione di cybersecurity

Il settore dell'energia è critico per la stabilità economica e la sicurezza nazionale, quindi è un obiettivo rilevante per gli hacker, che possono colpire con l'intento di estorcere denaro (cybercrime) o di compiere azioni dimostrative (hacktivism). Pensiamo che gli attacchi informatici rappresentino il rischio più grave per le aziende energy, in particolare per le Pmi, che possono contare su limitate risorse per la difesa. Molte delle tecnologie utilizzate nel settore energy sono inoltre integrate in reti più ampie, il che aumenta il rischio di un effetto domino in caso di violazioni della sicurezza.

È bene quindi che i decisori del settore siano informati in merito alle minacce e alle loro conseguenze: perdite economiche, derivanti dal furto di dati, dall'interruzione del servizio e delle attività di R&D, ma anche compromissione della reputazione pubblica dell'azienda.

Danni alla reputazione

Gli attacchi informatici, i furti di dati e le conseguenti interruzioni del servizio possono causare danni importanti non solo alla privacy dei clienti delle aziende vittime ma

anche all'immagine e alla reputazione delle stesse, causando la perdita di fiducia dei clienti e degli investitori. La sicurezza delle informazioni personali è un aspetto sempre più importante per i clienti, che vogliono essere sicuri che le loro informazioni personali, finanziarie o comunque sensibili non siano utilizzate impropriamente.

Allo stesso modo, incorrere in sanzioni per il mancato rispetto delle normative di sicurezza informatica e privacy possono comportare danni reputazionali significativi per l'azienda.

La conformità normativa

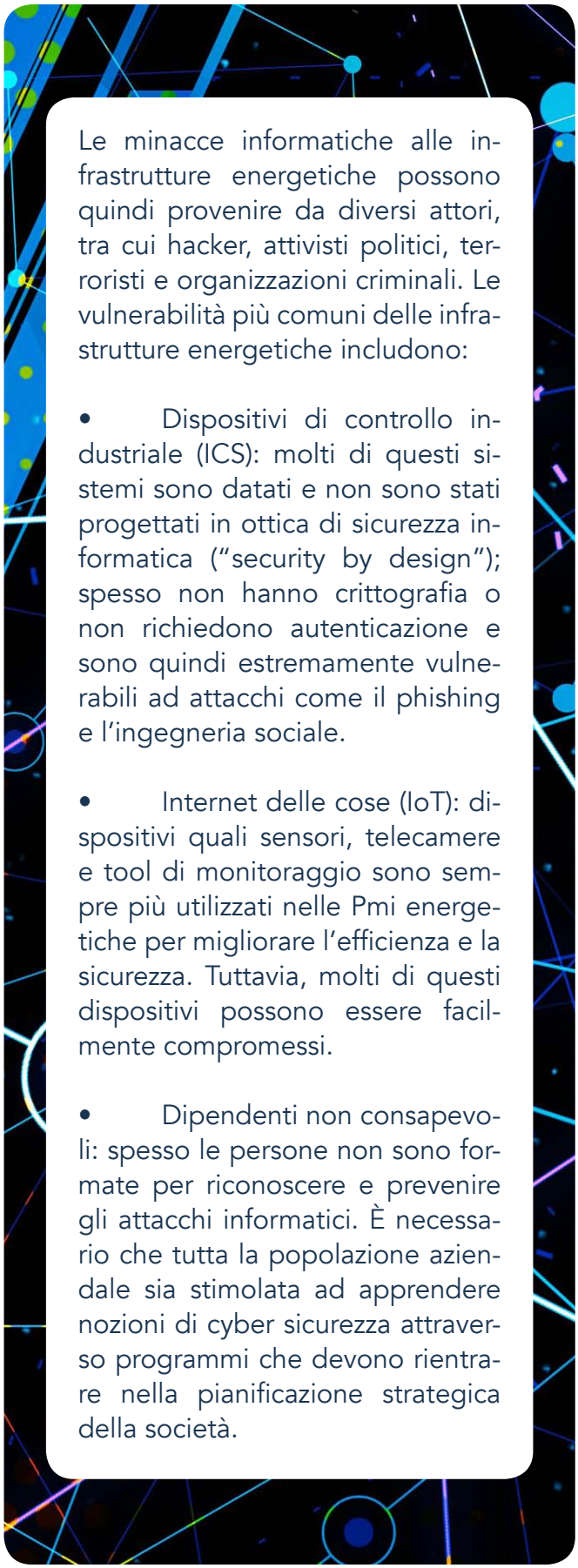
Le aziende del settore energy devono conformarsi a diverse normative sulla sicurezza informatica, come la Direttiva Nis (Network and Information Security) dell'Unione europea che richiede alle imprese di identificare e mitigare i rischi informatici, di monitorare le loro reti e di segnalare le violazioni della sicurezza informatica alle autorità competenti; oppure il Regolamento generale sulla protezione dei dati (Gdpr) che richiede alle aziende di proteggere i dati personali dei cittadini a loro affidati.

La mancata conformità può comportare multe decisamente salate e gravi sanzioni penali. Ad esempio, la violazione del Gdpr prevede penalità fino al 4% del fatturato annuo globale dell'azienda.

Le aziende del settore energetico devono quindi assicurarsi di implementare adeguate misure di sicurezza per proteggere le proprie infrastrutture, i dati personali di clienti e dipendenti, adottando misure di prevenzione adeguate.

Minacce informatiche e vulnerabilità

È chiaro che più i sistemi aziendali diventano tecnologicamente efficienti, più sono vulnerabili agli attacchi cyber.



Le minacce informatiche alle infrastrutture energetiche possono quindi provenire da diversi attori, tra cui hacker, attivisti politici, terroristi e organizzazioni criminali. Le vulnerabilità più comuni delle infrastrutture energetiche includono:

- Dispositivi di controllo industriale (ICS): molti di questi sistemi sono datati e non sono stati progettati in ottica di sicurezza informatica ("security by design"); spesso non hanno crittografia o non richiedono autenticazione e sono quindi estremamente vulnerabili ad attacchi come il phishing e l'ingegneria sociale.

- Internet delle cose (IoT): dispositivi quali sensori, telecamere e tool di monitoraggio sono sempre più utilizzati nelle Pmi energetiche per migliorare l'efficienza e la sicurezza. Tuttavia, molti di questi dispositivi possono essere facilmente compromessi.

- Dipendenti non consapevoli: spesso le persone non sono formate per riconoscere e prevenire gli attacchi informatici. È necessario che tutta la popolazione aziendale sia stimolata ad apprendere nozioni di cyber sicurezza attraverso programmi che devono rientrare nella pianificazione strategica della società.

Affrontare la situazione

Secondo il PWC Global Digital Trust Insights del 2023, due terzi dei dirigenti azienali considerano la criminalità informatica la minaccia più significativa nei prossimi dodici mesi. Per risolvere il problema dell'elefante nella stanza pensiamo sia necessario affrontare la situazione coinvolgendo partner tecnologici esperti di cybersecurity capaci di analizzare innanzi tutto le vulnerabilità del sistema informatico e identificare le misure necessarie per proteggerla. In molti casi, infatti, è sufficiente avere un quadro chiaro e aggiornato della situazione per rendersi conto che la stessa è gestibile in-house, con il supporto di un partner competente.

Ci sono tuttavia alcune sfide peculiari del settore energy che devono essere affrontate a monte:

- Dipendenza da tecnologie legacy: molte infrastrutture energetiche in Italia utilizzano tecnologie legacy che non sono state progettate per affrontare le attuali minacce informatiche. Ciò rende difficile l'aggiornamento delle infrastrutture e la loro protezione. Idealmente, la sicurezza informatica dovrebbe essere integrata già nella fase di progettazione delle infrastrutture energetiche.

- Mancanza di risorse: molte aziende energetiche sono piccole e medie imprese che non dispongono delle risorse necessarie per investire in soluzioni di sicurezza informatica avanzate.

- Poca consapevolezza lungo l'intera value chain: come abbiamo già evidenziato, molte aziende energetiche - soprattutto le più piccole - non sono consapevoli delle minacce informatiche e dei rischi che comportano. La sicurezza informatica deve essere un aspetto partecipato della cultura aziendale anche lungo l'intera filiera: se un elemento della value chain è impattato, ogni altro componente della stessa subirà delle ripercussioni.

L'impatto sulla filiera

Gli incidenti di sicurezza riguardanti le catene di approvvigionamento hanno rappresentato il 17% delle intrusioni nel 2021, rispetto a meno dell'1% nel 2020. Adottando un approccio consapevole alla cyber security lungo tutta la catena, si contribuisce alla sicurezza generale dell'intero Sistema-Paese.

Intelligence strategica: prevenzione, non reazione

È necessario adottare un approccio lungimirante e preventivo alla cybersecurity, che la integri nelle decisioni critiche sull'espansione aziendale. Il primo passo per fare questo è avere visibilità totale sulle attività degli utenti e sui punti deboli dell'infrastruttura IT dell'azienda.

La Network Detection and Response (Ndr)

La "Network Detection and Response" è dunque una soluzione di sicurezza informatica che consente di monitorare il traffico di rete e individuare le attività sospette all'interno del sistema aziendale. È una soluzione ottimale in quanto estremamente personalizzabile, chiara e integrabile. Grazie all'intelligenza artificiale, Ndr è in grado di individuare eventuali anomalie o comportamenti sospetti, emettendo nel caso un alert che consente al personale di sicurezza di intervenire in ottica preventiva.

La sicurezza del settore energetico è l'elefante che non possiamo ignorare, secondo Arte che, insieme a Professional Link, operatore di telecomunicazioni e fornitore di tecnologie di cybersecurity, ritiene urgente un cambio di mentalità che porti a riconoscere la sicurezza informatica come una priorità strategica.

La collaborazione a livello sistemico è sempre più diffusa nel settore utility, questo rende inoltre necessario proteggere le aziende non solo in quanto tali ma anche considerandole come parte di un sistema più ampio e complesso, composto da una pluralità di produttori, che deve essere difeso nella sua interezza.

È necessario chiederci cosa possiamo fare oggi per costruire infrastrutture adatte a rispondere ai pericoli di domani. Solo in questo modo il settore dell'energia in Italia potrà garantire la propria sicurezza e contribuire alla transizione energetica del Paese in modo sostenibile e sicuro.

Internet of things
L'Internet delle cose (IoT) può essere utilizzato per monitorare e controllare le infrastrutture energetiche in tempo reale, migliorando l'efficienza e la sostenibilità. Ad esempio, i sensori IoT possono essere utilizzati per rilevare le variazioni di temperatura e le perdite nei sistemi di riscaldamento e raffreddamento, riducendo così i costi energetici. Inoltre, i dispositivi IoT possono essere utilizzati per raccogliere dati sui consumi energetici degli edifici e delle strutture, consentendo ai gestori di ottimizzare l'uso dell'energia. Sostenibilità ed efficienza passano anche da un uso più consapevole dei dati.

Intelligenza Artificiale e Machine Learning
L'Intelligenza Artificiale (IA) e il Machine Learning (ML) possono essere utilizzati per analizzare grandi quantità di dati e migliorare l'efficienza delle infrastrutture energetiche. Ad esempio, l'IA può essere utilizzata per analizzare i dati sui consumi energetici degli edifici e delle strutture e identificare le aree in cui l'energia è usata in modo inefficiente. Inoltre, ML può essere utilizzato per prevedere i picchi di domanda, consentendo una pianificazione anticipata ed efficiente.

Blockchain
La blockchain può essere utilizzata per migliorare la trasparenza delle transazioni energetiche perché consente di creare una rete decentralizzata che registra tutte le transazioni di energia. Ciò può ridurre il rischio di frodi e manipolazioni dei dati, migliorando la fiducia tra i partecipanti del mercato dell'energia.

La soluzione Network Detection and Response si implementa in tre fasi:

1. network traffic analytics
2. detection
3. response

1. Network traffic analytics

La soluzione Ndr si compone di una Sonda e di un Server. La sonda, posizionata all'interno della rete dell'azienda (non importa quante siano le sedi), intercetta le comunicazioni che l'attraversano. Le informazioni sono inviate al server che esegue analisi sofisticate sui dati di traffico. Grazie a questa analisi è possibile conoscere chi ha generato traffico e in quale momento nel tempo, in quale modalità e con quali protocolli e il tipo di trasferimento effettuato. In una parola, si ha la totale visibilità. Questo permette di stabilire in modo preciso il livello di rischio a cui l'azienda è esposta.

2. **Detection**

Nella fase di Detection le informazioni ottenute dalla prima fase di analisi sono elaborate tramite Machine Learning, IA e behavioral analysis, determinando il livello di sicurezza dell'infrastruttura aziendale, le anomalie e le vulnerabilità al suo interno, gli eventuali attacchi subiti e, nel caso, la fase in cui l'attacco si trova.

3. Response

Nella fase di Response il server coordina in tempo reale la risposta all'attacco, istruendo le componenti di sicurezza a protezione dell'infrastruttura. Next Generation Firewalls, Client Edr e Ndr server operano sinergicamente per bloccare la minaccia e mitigare gli effetti di incidenti che hanno già compromesso la rete. L'automatizzazione del processo di Response comprime i tempi di reazione alle minacce, riducendo il perimetro di rischio e il carico di lavoro per i reparti IT.