Numero 3 - luglio 2025

L'OSINT NELL'AMBITO DELLA NIS 2

MIRKO LAPI

L'OSINT NELL'AMBITO DELLA NIS 2

Opportunità e minacce per le PMI: il valore dell'intelligence da fonti aperte nella cybersecurity e nella compliance aziendale

L'Open Source Intelligence (OSINT) è la pratica di raccogliere, analizzare e utilizzare informazioni provenienti da fonti aperte e pubblicamente disponibili. A differenza dell'intelligence tradizionale, l'OSINT sfrutta dati accessibili a chiunque (web, social media, documenti pubblici, registri, ecc.) senza ricorrere a metodi clandestini o illegali. Nel contesto della cybersecurity, l'OSINT consente di fotografare la propria "impronta digitale" e di capire quali informazioni su un'azienda (o un individuo) siano esposte pubblicamente, aiutando così a identificare minacce e vulnerabilità potenziali. Proprio al fine di individuare e rilevare tempestivamente segnali di attacco, sempre più organizzazioni (governative e private) adottano l'OSINT come parte integrante delle loro difese informatiche, affiancandolo alle tradizionali misure di sicurezza.

La NIS 2 è la direttiva UE sulla sicurezza delle reti e dei sistemi informativi (Network and Information Security Directive), entrata in vigore a livello europeo nel gennaio 2023. La direttiva amplia il campo di applicazione a nuovi settori critici e impone alle organizzazioni di medie e grandi dimensioni in questi ambiti di adottare una gestione del rischio approfondita e misure di protezione adeguate. L'obiettivo è uniformare verso l'alto il livello di cybersecurity in tutta l'UE, riconoscendo la sicurezza informatica come elemento critico per l'economia e la società digitale. Pur rivolta principalmente a entità medio-grandi, la NIS 2 tocca anche molte PMI oltre che micro e piccole imprese (ad esempio fornitori ICT o di sicurezza che servono soggetti essenziali, o aziende parte di filiere critiche che sono quindi coinvolte indipendentemente dalle dimensioni). In Italia, la direttiva è stata recepita ad ottobre 2024 e l'Agenzia per la Cybersicurezza Nazionale è l'Autorità nazionale competente NIS.

In sintesi, OSINT e NIS 2 convergono sul tema della cybersecurity: la prima fornisce metodologia e strumenti per raccogliere intelligence utile alla sicurezza, la seconda impone obblighi normativi di protezione e gestione del rischio. Di seguito vedremo come l'OSINT possa avere un ruolo strategico nell'aiutare le PMI a conformarsi alla direttiva NIS 2, quali opportunità offre e quali minacce presenta questa disciplina nel contesto aziendale attuale.

Mirko Lapi è Consulente e Formatore specializzato in Open Source Intelligence (OSINT), sicurezza delle informazioni e sviluppo del pensiero critico applicato ai processi decisionali. Ha prestato servizio nelle Forze Armate italiane per 27 anni, di cui 16 anni all'interno del II Reparto Informazioni e Sicurezza dello Stato Maggiore della Difesa, dove ha lavorato come analista presso il Centro Intelligence Interforze dello Stato Maggiore della Difesa e come docente di Intelligence presso il Centro Interforze di Formazione Intelligence (CIFIGE). È Professore a contratto di Open Source Intelligence (OSINT) presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Foggia. Inoltre, ricopre il ruolo di Professore a contratto di Cyber Security per il Corso di Laurea Magistrale in Ingegneria dei Sistemi Intelligenti presso la Facoltà di Ingegneria, Università Campus Bio-Medico di Roma.

IL RUOLO STRATEGICO DELL'OSINT NELLA CONFORMITÀ ALLA NIS 2

La direttiva NIS 2 obbliga le organizzazioni a dotarsi di un solido **framework di gestione del rischio cyber** e di misure tecniche/organizzative efficaci. In questo contesto, l'OSINT si rivela uno strumento strategico per supportare la compliance: attraverso la raccolta sistematica di informazioni su minacce, vulnerabilità e trend di attacco, l'OSINT alimenta il processo di **risk management** con dati aggiornati e concreti.

Ad esempio, utilizzare fonti aperte per monitorare nuove vulnerabilità di sicurezza, indicatori di compromissione o attività anomale consente di identificare preventivamente rischi emergenti e di attuare controlli mitigativi prima che si verifichino incidenti.

Questo approccio proattivo alle minacce informatiche promosso dalla NIS 2 permette alle PMI di non limitarsi ad una difesa reattiva, ma di giocare d'anticipo, riducendo la probabilità e l'impatto degli attacchi informatici.

Un altro aspetto chiave della NIS 2 è il coinvolgimento della governance aziendale nella sicurezza: il tema cyber deve essere integrato nella cultura organizzativa, con responsabilità chiare, politiche e procedure ad hoc e formazione continua del personale. Anche qui l'OSINT gioca un ruolo importante: i dati raccolti da fonti aperte possono fornire insight preziosi al management su minacce settoriali, vulnerabilità dei propri sistemi o fornitori, e trend di attacco. Includere l'analisi OSINT nei report periodici al top management significa avere decisioni informate e basate sull'intelligence, rafforzando così la governance della sicurezza. Inoltre, OSINT e Cyber Threat Intelligence possono facilitare la condivisione di informazioni sulle minacce con le autorità e i CSIRT, proprio come richiesto da NIS 2.

Dal punto di vista della compliance normativa interna, l'OSINT trova collegamenti anche con il modello organizzativo previsto dal D.Lgs. 231/2001 (responsabilità amministrativa degli enti).

Tale modello impone alle imprese di identificare e prevenire i reati presupposto – tra cui oggi rientrano vari reati informatici – mediante adeguati protocolli e controlli.

In un sistema di gestione dei rischi come quello 231, la sicurezza IT è ormai un ambito di massima attenzione.

Cybersecurity e modello 231 sono <u>inevitabilmente connessi</u>: un grave attacco informatico subito per carenze organizzative potrebbe esporre l'azienda a responsabilità.

Inserire l'OSINT tra le misure di prevenzione significa quindi dotarsi di una **capacità in più per e reagire prontamente**.

Ad esempio, un organismo di vigilanza 231 potrebbe avvalersi di report OSINT periodici per verificare se circolano in rete informazioni su possibili attacchi all'azienda, data leak o altri elementi critici, e sollecitare tempestive segnalazioni alle autorità competenti (laddove previste) o interventi correttivi prima che il rischio si concretizzi. In quest'ottica, l'OSINT rafforza la due diligence dell'azienda sul fronte cyber e contribuisce a dimostrare l'adozione di misure organizzative diligenti sia verso NIS 2 sia verso ulteriori obblighi di legge nazionali.

In definitiva, l'OSINT funge da "sensore" nel sistema di sicurezza delle PMI: supporta la conformità alla NIS 2 fornendo informazioni utili per il risk management e la governance, e allo stesso tempo si inserisce armonicamente nei modelli di compliance esistenti (231, GDPR, etc.) assicurando un presidio aggiuntivo sul rischio informatico.

L'azienda che investe in OSINT dimostra una postura proattiva, trasformando un obbligo normativo (proteggersi dai cyber attacchi) in un'opportunità per migliorare conoscenza e controllo del proprio ecosistema digitale

L'OSINT: OPPORTUNITA' PER LE PMI

Per le piccole e medie imprese, adottare pratiche di OSINT può tradursi in numerosi vantaggi concreti. In particolare, le principali opportunità includono:

- **Monitoraggio di minacce e vulnerabilità nel proprio settore**: l'OSINT consente di tenere d'occhio in tempo reale ciò che accade nell'ecosistema cyber relativo al settore di business dell'azienda. Ad esempio, è possibile monitorare costantemente forum, social media, portali specializzati e persino il dark web alla ricerca di **segnali di nuove minacce emergenti**, come vulnerabilità software appena scoperte, campagne di malware o phishing mirate a determinate categorie di aziende. Ciò permette alla PMI di sapere tempestivamente se, ad esempio, è emerso un nuovo exploit che riguarda i sistemi utilizzati, così da intervenire prontamente con *patch* o altre misure di mitigazione. Inoltre, mediante OSINT si possono **rilevare attività sospette o indicatori di preparativi di attacco**, profilando anche potenziali aggressori (es. gruppi hacker noti per colpire un certo settore) con relative tattiche, tecniche e procedure (TTP). Tutto ciò rafforza la capacità preventiva e di *early warning* dell'azienda.
- **Analisi della concorrenza e delle strategie di mercato:** al di là della sicurezza, le tecniche OSINT possono fornire valore anche al business in senso stretto. Molte informazioni pubbliche sulle aziende concorrenti – dai siti web ai social, fino agli annunci di lavoro o alle pubblicazioni – possono essere raccolte e analizzate per **ottenere *insight* strategici**. Ad esempio, l'OSINT permette (sempre nei limiti del lecito) di osservare le mosse dei competitor, capire attraverso indizi pubblici quali nuovi prodotti o servizi stiano sviluppando, come comunicano con i clienti, quali partnership instaurano. Può servire per effettuare ricerche di mercato mirate e individuare i trend del settore. Per una PMI, queste informazioni open source sono un modo relativamente economico per colmare gap informativi e supportare decisioni di business. Inoltre, utilizzare internamente l'OSINT accresce la **consapevolezza cyber**: analizzando le informazioni disponibili su di sé e sugli altri, l'azienda matura una migliore percezione della propria postura digitale e di come eventualmente migliorarla.
- **Protezione della brand reputation e prevenzione delle frodi**: la reputazione online è un asset cruciale anche per le PMI, influenzando la fiducia di clienti, partner e stakeholder.

L'OSINT offre gli strumenti per condurre un'attività di *due diligence* reputazionale continua, ovvero per monitorare il web alla ricerca di contenuti che citano l'azienda, i suoi prodotti o esponenti, così da intercettare sul nascere potenziali crisi reputazionali. Monitorando blog, news, recensioni, forum e social, l'azienda può individuare tempestivamente lamentele o notizie negative e reagire prima che diventino virali. Allo stesso modo, può consentire l'individuazione di **violazioni della proprietà intellettuale o uso improprio del brand**, ad esempio loghi o marchi usati senza autorizzazione, oppure la presenza di **profili falsi e siti di phishing** che imitano l'azienda. Queste attività consentono di prevenire truffe ai danni dei clienti (es. fake shop online con il nome del brand) e attacchi di social engineering verso i dipendenti. Infine, nel corso di operazioni straordinarie (es: fusioni e acquisizioni) l'OSINT è utile per valutare la reputazione e l'affidabilità dei potenziali partner o degli asset da acquisire, raccogliendo informazioni pubbliche che potrebbero evidenziare possibili criticità.

In estrema sintesi, l'OSINT mette a disposizione delle PMI, a costo contenuto, informazioni che consentono di migliorare la conoscenza del contesto nel quale operano. Dal fronte della cybersecurity preventiva (minacce, vulnerabilità, attori malevoli) a quello della business intelligence (concorrenza, mercato, reputazione), le fonti aperte rappresentano un importante valore aggiunto. Saper sfruttare l'OSINT consente alle PMI di **colmare il divario di risorse rispetto alle grandi aziende**, aumentando la resilienza e la competitività con mezzi efficaci e mirati.

L'OSINT: RISCHI PER LE PMI

Se da un lato, come abbiamo visto, l'OSINT presenta molteplici opportunità, dall'altro insistono alcuni rischi che le PMI devono conoscere, al fine di saperli gestire adeguatamente. Ecco quindi i principali pericoli legati all'OSINT in ambito aziendale:

- **Rischio di esposizione di informazioni sensibili:** l'OSINT, per sua natura, porta alla luce tutto ciò che è pubblicamente accessibile. Ciò significa che eventuali dati aziendali sensibili lasciati esposti online (intenzionalmente o per errore) potranno essere facilmente individuati – non solo dall'azienda stessa, ma anche da attori ostili. Un caso tipico è quello di servizi o dispositivi connessi alla rete ma non protetti a dovere: esistono motori di ricerca specializzati (es. Shodan) che consentono a chiunque di scoprire **router con backdoor aperte, telecamere di sorveglianza non protette o persino sistemi di controllo industriale con password di default**. Tali strumenti fanno sì che una cattiva configurazione di sicurezza diventi immediatamente visibile su Internet, trasformando la rete in un "terreno fertile" per i cybercriminali. Ciò significa che, attraverso tipiche tecniche di OSINT, eventuali errori o leggerezze (come server lasciati aperti, credenziali hard-coded pubblicate in un repository, dipendenti che condividono troppe informazioni su LinkedIn) possono essere scoperti e sfruttati anche da potenziali aggressori.

Uso improprio dell'OSINT da parte di attori malevoli: l'OSINT è un'arma a doppio taglio: la stessa trasparenza informativa che supporta la fase difensiva, favorisce anche chi intende attaccare. Ancor di più se l'azienda non monitora la propria esposizione online. L'OSINT è quindi uno strumento utile per i difensori, ma lo è altrettanto per i criminali informatici. Ad esempio, durante la fase di ricognizione (reconnaissance) di un attacco un aggressore può raccogliere dalle fonti aperte dettagli sull'organigramma di un'azienda, sui fornitori, sulle tecnologie utilizzate, sulle abitudini dei dipendenti, e usare tali informazioni per pianificare attacchi su misura. Anche studiare i profili social dei dipendenti e i contenuti condivisi pubblicamente potrebbe rivelare punti deboli per attacchi di social engineering: conoscendo nomi, ruoli, email e interessi di una persona, un phisher può confezionare una finta email mirata e convincente (spear phishing) e indurre il destinatario inconsapevole a cedere credenziali di accesso o cliccare su un malware. Allo stesso modo, informazioni disseminate online per marketing o trascuratezza (ad es. screenshot di software aziendali, listini, manuali tecnici) possono fornire indicazioni su come penetrare nei sistemi. L'OSINT dunque amplifica la superficie di attacco: ciò che l'azienda comunica (o fa trapelare) pubblicamente può diventare un'arma nelle mani dei cybercriminali.

Le PMI, spesso meno protette, sono bersagli appetibili e devono essere consapevoli che concorrenti scorretti o gruppi criminali possono svolgere attività di OSINT su di loro, anche facendo emergere informazioni imbarazzanti o negative (si pensi a cause legali, recensioni pessime, dati finanziari in sofferenza) da sfruttare a loro vantaggio.

Rischi di conformità normativa e aspetti legali: sebbene l'OSINT si basi su fonti aperte, la sua pratica non è esente da considerazioni legali. Chi conduce attività OSINT deve assicurarsi di rispettare la privacy e i dati personali di terzi, nonché di non violare termini di servizio di piattaforme online o leggi sul diritto d'autore. Ad esempio, raccogliere sistematicamente dati personali pubblicati in rete (nomi, foto, profili) può confliggere con la normativa GDPR se tali dati sono usati per finalità diverse da quelle per cui erano stati pubblicati. Le aziende devono quindi adottare misure adeguate per garantire la conformità alle leggi sulla privacy nell'utilizzo dell'OSINT. È fondamentale trovare un equilibrio tra l'uso legittimo delle informazioni aperte e la tutela dei diritti degli individui coinvolti. Inoltre, le informazioni raccolte via OSINT potrebbero essere inaccurate o fuorvianti: fare affidamento su dati non verificati può portare a valutazioni errate. Da qui la necessità di validare sempre le fonti (ad es. usando più riscontri) per evitare il rischio di disinformazione. In termini legali, va considerato anche **il limite tra OSINT e attività investigative.** Le PMI devono quindi definire chiaramente policy etiche e procedurali per l'OSINT, **formando il personale a cosa è lecito fare e cosa no**.

Un uso improprio o negligente dell'OSINT può esporre l'azienda a sanzioni (privacy, 231) o a danni reputazionali, per cui è essenziale approcciare questa disciplina con rigore e consapevolezza dei confini normativi.

L'OSINT: ESEMPI DI APPLICAZIONE

Le modalità di impiego dell'OSINT possono variare a seconda del settore in cui opera l'organizzazione, con specifiche declinazioni legate al tipo di minacce prevalenti e di informazioni utili disponibili.

Vediamo ora, a titolo esemplificativo, alcune applicazioni concrete nel settore energetico e nel settore bancario.

Il Settore Energetico

Le imprese del comparto energetico (es. fornitori di elettricità, gas, petrolio, operatori di rete) rientrano tra le infrastrutture critiche essenziali su cui la NIS 2 impone obblighi stringenti. Il motivo è chiaro: un attacco informatico riuscito a una centrale elettrica o a un gestore di distribuzione può avere conseguenze sistemiche gravissime. Non a caso, a livello globale il settore energetico risulta tra i più interessati dagli attacchi informatici alle infrastrutture critiche. In questo contesto, l'OSINT diventa un alleato prezioso per aumentare la resilienza cyber. I team di sicurezza delle aziende energetiche possono utilizzare fonti aperte per monitorare costantemente le minacce specifiche: ad esempio seguendo blog e bollettini di sicurezza (CSIRT, vendor, ecc...) per essere informati su nuove vulnerabilità di sistemi SCADA/ICS ampiamente utilizzati nel settore, oppure monitorando forum clandestini e community al cui interno potrebbero circolare indicazioni su possibili attacchi a impianti energetici.
Strumenti come il già citato Shodan – definito il "Google" dei dispositivi IoT/ICS – vengono impiegati per effettuare scansioni mirate delle proprie reti industriali, verificando la presenza di dispositivi che non dovrebbero essere visibili pubblicamente o con porte aperte non necessarie.
In tal modo, l'azienda può correggere configurazioni errate prima che qualcuno ne approfitti.

Infine, l'OSINT supporta anche nella gestione delle crisi: in caso di blackout o incidente, le notizie sui social e media locali possono fornire indicazioni immediate sull'estensione e l'impatto, aiutando a orientare la risposta. In sintesi, per il settore energetico l'OSINT è uno strumento cruciale sia preventivo (hardening* proattivo di sistemi, Threat Intelligence) sia reattivo (*situational awareness* durante gli incidenti), e rappresenta un tassello importante per soddisfare le richieste di NIS 2 in termini di sorveglianza del rischio e scambio informativo.

**L'hardening è un insieme di operazioni specifiche di configurazione di un sistema informatico, finalizzate a minimizzare l'impatto di possibili attacchi informatici che sfruttano vulnerabilità del sistema, migliorandone così la sicurezza complessiva.*

Il Settore Bancario-Finanziario

Banche, assicurazioni e società finanziarie sono tradizionalmente bersagli privilegiati dei cyber criminali, attirati sia dal potenziale guadagno economico sia dalla rilevanza sistemica di questi enti. Di conseguenza, il settore *Banking & Finance* ha sviluppato da tempo capacità di intelligence proprie e oggi l'OSINT vi gioca un ruolo sempre più strategico. Un utilizzo fondamentale è il **rilevamento di frodi e attacchi finanziari**: attraverso l'analisi di informazioni pubbliche, una banca può **individuare segnali anticipatori** di possibili campagne di attacco o schemi di frode in preparazione. Ad esempio, monitorando costantemente i *dump* di data breach pubblicati nel sottobosco del web, si potrebbero individuare tracce di **credenziali violate** appartenenti a clienti o dipendenti della banca, così da attivare misure (reset password, allerte) prima che vengano sfruttate dai criminali. Oppure, l'analisi di conversazioni sui social media e forum potrebbe far emergere informazioni su **attività sospette di potenziali truffatori**, come soggetti che offrono servizi illegali collegati a conti bancari, phishing kit in vendita, ecc...

Le banche utilizzano l'OSINT anche per il contrasto al riciclaggio di denaro e al finanziamento del terrorismo e in contesti ad alto rischio (es. paesi sotto sanzioni) può supportare la verifica di notizie pubbliche su società o individui e può consentire di individuare attività illecite.

Dal punto di vista della cyber difesa "pura", le strutture finanziarie integrano OSINT nel loro SOC/CSIRT per arricchire la *Threat Intelligence*: le informazioni su nuove varianti di un malware bancario, su campagne di phishing mirato, su vulnerabilità nei sistemi di home banking vengono raccolte da fonti aperte (report di società di sicurezza, gruppi Telegram di hacker, etc.) e subito trasformate in indicatori da caricare nei sistemi di monitoraggio interno. **Proattività** è la parola chiave: l'OSINT consente infatti un approccio prudenziale e proattivo nella mitigazione delle minacce. Anche la protezione dei clienti beneficia dell'OSINT: molte banche inviano alert se in rete compaiono elenchi di carte di credito rubate o IBAN contraffatti; ciò è possibile perché hanno task force che monitorano regolarmente il web in cerca di questi dump e li incrociano con le proprie basi dati.

COME LE PMI POSSONO IMPLEMENTARE L'OSINT IN CONFORMITÀ ALLA NIS 2

Dato il valore strategico dell'OSINT, anche le PMI – pur con risorse limitate – possono e dovrebbero integrarla nelle proprie pratiche di cybersecurity.

Ecco alcuni consigli su **come implementare efficacemente l'OSINT** in relazione alla NIS 2:

Strumenti OSINT consigliati per le PMI: oggi esistono numerosi tool, molti dei quali gratuiti o open source, che permettono di svolgere attività OSINT senza grandi investimenti. Ad esempio, motori di ricerca specializzati (vds Shodan) che consentono di scoprire quali asset della propria azienda sono visibili online e con quali porte/aperture (utile per trovare server o dispositivi esposti involontariamente).

Piattaforme come Have I Been Pwned permettono di verificare se indirizzi email aziendali sono coinvolti in data breach noti, segnalando potenziali compromissioni di account. Strumenti commerciali integrati consentono poi di automatizzare la raccolta di informazioni da decine di fonti (DNS, social media, database pubblici) e offrono visualizzazioni grafiche delle relazioni trovate, facilitando analisi anche complesse. Per il monitoraggio del brand e delle conversazioni online, si possono impostare avvisi con Google Alerts o utilizzare piattaforme di social listening. Molti di questi strumenti ricalcano tecniche che i cybercriminali già usano contro le aziende, ma in termini difensivi consentono di "**osservare con gli occhi dell'attaccante** e risolvere le vulnerabilità prima che vengano sfruttate.

È importante che la PMI selezioni pochi strumenti mirati, adatti alle proprie esigenze (ad es. focalizzati sul proprio settore), e ne faccia un uso costante integrandoli nei processi di sicurezza.

Best practice per un uso efficace e sicuro: introdurre l'OSINT in azienda richiede l'adozione di alcune buone pratiche.

Primo, definire gli obiettivi: capire se si vuole usare OSINT per scopi prevalentemente difensivi (threat intelligence, vulnerability assessment) o anche per market intelligence e delimitare il perimetro (quali informazioni cercare, con quali frequenze).

Secondo, verificare l'affidabilità delle fonti: l'OSINT genera grandi quantità di dati, ma non tutti sono accurati o rilevanti. È essenziale implementare procedure di validazione rigorose, incrociando le informazioni da più fonti e valutandone la credibilità. Ciò migliora significativamente l'affidabilità delle informazioni utilizzate nelle strategie di sicurezza, mitigando anche i rischi di disinformazione.

Terzo, rispettare la legalità e l'etica: il team OSINT deve operare solo su dati pubblici e liberamente accessibili, astenendosi da ogni tentativo di intrusione o violazione di sistemi (che trasformerebbe l'OSINT in hacking attivo, fuori dal lecito). Occorre inoltre evitare di raccogliere dati personali non necessari e comunque trattarli in conformità al GDPR e alle normative privacy applicabili. Se ad esempio si effettua OSINT su un individuo (es. per assumere un dipendente o valutare un partner), bisogna attenersi ai limiti della due diligence e non pubblicare o conservare indebitamente informazioni eccedenti lo scopo (*si veda l'articolo n.2 marzo 2025 - L'OSINT, Strumenti, limiti e best practice in ambito aziendale e nelle investigazioni private*). Una buona pratica è **predisporre un codice interno** per le attività OSINT, che copra aspetti di riservatezza, etica e rispetto delle leggi.

Formazione e sensibilizzazione del personale: la riuscita di un programma OSINT in una PMI dipende dalle competenze delle persone coinvolte. È consigliabile identificare e formare specificamente uno o più addetti (ad esempio membri del team IT/security) sulle tecniche OSINT e sui tool selezionati. Il personale deve essere adeguatamente formato sulle tecniche di ricerca, verifica e analisi delle informazioni raccolte. Esistono corsi e risorse online sull'OSINT che possono elevare rapidamente le capacità interne.

Oltre agli specialisti, è poi utile fare **sensibilizzazione** più ampia in azienda: far capire a tutti i dipendenti che le informazioni che condividono pubblicamente (sui social, nei convegni, ecc.) possono essere utilizzate per compiere attacchi. Promuovere una cultura dove ognuno è attento a cosa divulga (senza per questo limitare le attività di business) riduce la superficie di attacco sfruttabile via OSINT dagli avversari. Ad esempio, formare HR e marketing a non pubblicare dettagli tecnici troppo specifici nelle job description o nei case study pubblici può evitare di regalare indicazioni utili a potenziali attaccanti. Infine, la PMI può valutare di farsi affiancare da **consulenti esterni esperti in OSINT, specialmente nelle fasi iniziali di implementazione: questo garantisce un avvio corretto e conforme, trasferendo know-how allo staff interno.** Man mano che l'OSINT diventa parte integrante dei processi (es. controllo fornitori, analisi dei rischi periodica), l'azienda guadagnerà autonomia. Integrare l'OSINT significa anche prevedere momenti fissi – ad esempio durante gli audit di sicurezza o le riunioni *ad hoc* – in cui discutere le informazioni emerse e decidere eventuali azioni correttive. In questo modo, l'OSINT non resta un mero esercizio teorico ma produce cambiamenti tangibili nella postura di sicurezza e nella compliance aziendale.

PROSPETTIVE FUTURE

L'OSINT si conferma dunque un tassello di valore nel mosaico della cybersecurity per le PMI, specialmente nell'era della NIS 2 che richiede un approccio strutturato e proattivo alla gestione del rischio. In futuro, il peso dell'OSINT è destinato a crescere ulteriormente: la quantità di dati pubblici continua ad aumentare in modo esponenziale, e con essa la necessità di **filtrarli e sfruttarli intelligentemente**. Le nuove tecnologie – in particolare l'Intelligenza Artificiale – stanno dando ulteriore vigore all'OSINT, automatizzando la raccolta e l'analisi di enormi mole di informazioni.

Già oggi strumenti di OSINT evoluti integrano algoritmi di machine learning per identificare pattern sospetti in rete o per scandagliare il dark web in maniera estremamente efficace. Questo significa che anche le PMI potranno beneficiare di insight sempre più accurati. Sul fronte normativo, è plausibile che l'**attuazione di NIS 2** e di future regolamentazioni in materia di cybersecurity e tutela dei dati spingerà le aziende – grandi e piccole – ad adottare in modo più diffuso pratiche OSINT. La direttiva stessa enfatizza l'importanza delle attività di *monitoring, detection* e *analysis* nel ciclo di protezione; attività che trovano nell'OSINT un alleato naturale. Possiamo attenderci, come è auspicabile, una maggiore formalizzazione della **condivisione di informazioni** finalizzata a scambiare segnalazioni di minacce in tempo reale, rafforzando così la sicurezza collettiva.

In prospettiva, l'OSINT non sarà più visto solo come una disciplina "di nicchia", ma diventerà parte integrante dei **processi aziendali di *decision making* e compliance**. Dal supportare la scelta di un fornitore (verificando la sua reputazione online) al contribuire alla valutazione annuale dei rischi ICT, l'intelligence da fonti aperte si configurerà come un processo essenziale nelle attività di governance. Le PMI più lungimiranti coglieranno questo trend come un'opportunità per **accrescere la propria maturità digitale**: investire nell'OSINT significa adottare un approccio conoscitivo, data-driven, che può dare frutti non solo in termini di sicurezza (prevenzione di attacchi) ma anche di **vantaggio competitivo**. Immaginiamo ad esempio una piccola impresa manifatturiera che, grazie all'OSINT, scopre anticipatamente un cambiamento normativo o un nuovo standard nel proprio settore divulgato su fonti pubbliche internazionali: potrà adeguarsi prima delle altre. Oppure, un'azienda che individua tramite OSINT una nicchia di mercato emergente dalle discussioni online potrà, di conseguenza, orientare la propria strategia di business .

In conclusione, OSINT e NIS 2, indicano alle PMI la stessa direzione: quella di una **cybersecurity più consapevole, informata e collaborativa**. Le sfide non mancano – dalle complessità tecniche ai rischi legali – ma gli strumenti per affrontarle ci sono ed è quindi possibile **trasformare gli obblighi di legge in occasioni di miglioramento.** L'OSINT, con le sue opportunità e i suoi rischi ben governati, può supportare le PMI consentendo di non subire passivamente le norme ma anzi traendone slancio per innovare in sicurezza.

In un mondo in cui è sempre più valido l'assunto che "sapere è potere", coltivare la capacità di produrre conoscenza attraverso le fonti aperte rappresenta la chiave per costruire imprese resilienti, competitive e *compliant*