Martedì 27 Gennaio 2026
Notizie mercati esteri [1]

Cybersecurity e Direttiva NIS2: Opportunità Strategica per le Aziende Italiane nel Mercato Polacco

La Direttiva NIS2 trasforma la sicurezza informatica in vantaggio competitivo. Scopri come accedere ai finanziamenti UE di 6,2 miliardi di euro e posizionarti strategicamente nel mercato IT e Cybersecurity polacco in espansione.

Contesto Normativo e Opportunità di Mercato in Polonia

La **Direttiva NIS2** (Network and Information Systems Directive 2022/2555) rappresenta un punto di svolta nella governance della cybersicurezza europea. Entrata in vigore il 16 gennaio 2023, la direttiva mira a **elevare i standard di sicurezza informatica** per le infrastrutture critiche e i servizi essenziali in tutto il territorio UE. La Polonia, come membro dell'UE, è tenuta alla trasposizione delle disposizioni di NIS2, sebbene il processo di implementazione sia ancora in corso.

La **Commissione Europea** ha positivamente valutato il 29 ottobre 2025 il **terzo pagamento da 6,2 miliardi di euro** della Facility per la Ripresa e la Resilienza (RRF) alla Polonia, che è stato erogato il 30 novembre 2025, portando i fondi erogati finora a **26,9 miliardi di euro**. Di questi fondi KPO**, il 21,3%** è destinato alla **transizione digitale, che include investimenti in cybersicurezza, protezione infrastrutturale e implementazione di ISMS**. Ciò rappresenta un'opportunità strategica straordinaria per le aziende italiane che operano nel settore della sicurezza informatica. I finanziamenti KPO costituiscono un meccanismo diretto per sostenere investimenti in conformità normativa e protezione infrastrutturale, creando una domanda strutturale di soluzioni di sicurezza avanzate. Per le imprese italiane, l'accesso a questi fondi attraverso partnership con operatori polacchi e strutture pubbliche locali rappresenta un canale di crescita tangibile e prevedibile nel breve-medio termine.

Cybersicurezza come Priorità Strategica della Polonia nel 2026

La Polonia occupa una **posizione geopolitica critica** nel panorama europeo. A seguito del conflitto ucraino e della crescente pressione russa, il governo polacco ha identificato la cybersicurezza come una **priorità nazionale non negoziabile**. Nel **settembre 2025**, la Polonia ha annunciato l'allocazione di **1 miliardo di euro** per la cybersicurezza nel 2025, rappresentando un aumento del 67% rispetto ai 600 milioni di euro del 2024.

Il paese è attualmente sotto attacco sistemico da parte di entità sponsorizzate da stati ostili e cyber criminali. Secondo fonti governative, la Polonia subisce **molteplici tentativi di attacco al giorno** contro infrastrutture critiche. Le infrastrutture colpite includono ospedali, sistemi idrici municipali, reti energetiche e sistemi di trasporto. Sebbene la Polonia abbia respinto la stragrande maggioranza di questi attacchi, alcune operazioni hanno avuto successo, causando interruzioni di servizio e compromissioni di dati sensibili.

Questa situazione crea un **vuoto competitivo critico** all'interno della Polonia stessa. Le competenze locali di cybersicurezza, sebbene in espansione, rimangono insufficienti rispetto alla velocità di modernizzazione richiesta. **Le aziende italiane**, con una tradizione consolidata di expertise in conformità normativa, soluzioni integrate e certificazioni internazionali riconosciute, sono posizionate idealmente per colmare questo gap. Le imprese italiane possono offrire non solo tecnologie avanzate, ma anche gestione del rischio enterprise-grade e supporto alla compliance normativa—competenze che la Polonia necessita urgentemente.

Il Mercato Polacco della Cybersicurezza: Dimensioni e Traiettorie di Crescita

Il mercato della cybersicurezza in Polonia sta vivendo una **fase esplosiva di crescita**. Secondo le ricerche di mercato più recenti, il mercato è stato valutato a **1,8-2,29 miliardi di USD (1,54-1,96 miliardi di EUR) nel 2024** e si proietta di raggiungere **4,13-5 miliardi di USD (3,54-4,28 miliardi di EUR) entro il 2032**, con un **CAGR (Compound Annual Growth Rate) di 8,80-12%** nel periodo 2025-2032.

I driver di questa crescita sono molteplici e strutturali:

- **Trasformazione digitale accelerata** — il numero di imprese polacche che adottano soluzioni cloud, IoT e AI è in aumento esponenziale
- **Aumento delle minacce cyber** — il numero di incidenti di cybersicurezza segnalati è cresciuto del **45%** nel 2023 rispetto al 2022, con perdite finanziarie stimate a **2,8 miliardi di PLN (0,67 miliardi di EUR)**;
- **Conformità normativa obbligatoria** — la transposizione di NIS2 richiede investimenti sistemici in information security management systems (ISMS), incident reporting e supply chain security;
- **Supporto governativo consistente** — l'allocazione di risorse pubbliche per la modernizzazione infrastrutturale garantisce continuità della domanda.

I **settori prioritari** per gli investimenti in cybersicurezza in Polonia includono: *Energia* (incluso il settore nucleare in espansione), *Settore Finanziario e Bancario*, *Sanità e Strutture Ospedaliere*, *Trasporti e Logistica*, e *Produzione*. Ogni settore è classificato come "essenziale" o "importante" secondo le disposizioni di NIS2, con obblighi di conformità differenziati.

La **concentrazione di investimenti è maggiore nelle aree urbane centrali** (Varsavia, Cracovia, ?ód?), dove si trovano la maggior parte delle istituzioni finanziarie, degli ospedali di rilievo e dei nodi di trasporto strategici.

Come le Aziende Italiane Possono Posizionarsi

Le **aziende italiane operanti nel settore della cybersicurezza posseggono vantaggi competitivi distintivi** che le rendono particolarmente attraenti per il mercato polacco.

In primo luogo, **l'expertise italiana in conformità normativa** è consolidata e riconosciuta a livello internazionale. Le aziende italiane hanno accumulato decenni di esperienza nell'implementazione del GDPR, della Direttiva NIS originaria, e ora della NIS2. Questa expertise consente di offrire **soluzioni end-to-end di risk management e compliance**, non limitandosi a meri strumenti tecnologici, ma fornendo anche governance strutturale e supporto amministrativo.

In secondo luogo, le aziende italiane detengono **certificazioni internazionali di alto valore**, tra cui ISO/IEC 27001:2022 per la gestione della sicurezza informatica, ISO 27032 per la cybersecurity governance, e sempre più spesso il marchio QC1 dell'ACN, che può fungere da leva di credibilità, anche se il suo riconoscimento formale in Polonia è ancora in fase di sviluppo. Queste certificazioni forniscono **garanzie di qualità e conformità normativa** che riducono il rischio percepito dai clienti polacchi e facilitano l'accesso ai finanziamenti pubblici.

Terzo, le aziende italiane possono sviluppare **modelli di accesso al mercato polacco** altamente flessibili:

- **Partnership Strategiche con Provider Locali Polacchi** — identificare integratori di sistemi polacchi, consulenti e fornitori di servizi gestiti per distribuire soluzioni italiane adattate al contesto locale;
- **Joint Venture e Filiali Locali** — costituire entità giuridiche polacche controllate per accedere ai finanziamenti KPO e per avere una presenza operativa duratura;
- **Servizi di Consulenza e Governance** — offrire servizi di valutazione del rischio, audit di conformità a NIS2, e design di architetture di sicurezza adattate ai settori critici polacchi;
- **Soluzioni SaaS Verticali** — sviluppare piattaforme software as a service specifiche per i settori energetico, sanitario e finanziario polacco, con localizzazione del servizio e conformità ai requisiti di residenza dei dati stabiliti dalla Polonia.

I **settori prioritari di ingresso** rimangono l'Energia (con il sottosettore nucleare in crescita), il Settore Finanziario (banche e istituti di pagamento), la Sanità (ospedali e strutture di tele-medicina), e il Trasporto (porto di Danzica, ferrovia, aviazione). Per ciascun settore, il governo polacco ha identificato competenti authorities specifiche (es., il Ministero dell'Energia per il settore energetico, il Ministero della Salute per la sanità, la Banca Centrale Polacca per il settore finanziario), facilitando l'identificazione di interlocutori istituzionali per negoziazioni commerciali.

Strumenti di Finanziamento per le Aziende Italiane in Polonia

La **disponibilità di strumenti finanziari è uno dei principali catalizzatori di opportunità** per le aziende italiane che desiderano investire o operare in Polonia. I meccanismi di finanziamento si articolano su più livelli:

1. Fondi KPO Dedicati alla Cybersicurezza. Il **21,3% del totale KPO della Polonia** (pari a circa **12,8 miliardi di euro** dall'allocazione complessiva di 59,8 miliardi) è destinato alla transizione digitale, che include esplicitamente investimenti in cybersicurezza, protezione infrastrutturale e implementazione di ISMS. Le aziende italiane possono accedere a questi fondi attraverso:

- **sub-contratti con enti pubblici polacchi** (comuni, istituzioni centrali) che ricevono finanziamenti KPO;
- **partnership con aziende locali polacche** che, a loro volta, sono beneficiari di KPO;
- **investimento diretto in entità giuridiche** costituite in Polonia e registrate presso le autorità competenti.

2. Programmi di Incentivi Fiscali e di Credito Locale. Il governo polacco offre **esenzioni fiscali dal 15% al 50%** per investimenti in aziende che operano in settori strategici, inclusa la cybersicurezza, attraverso il **Polish Investment Zone (PSI)**. Inoltre, sono disponibili **prestiti bancari agevolati** erogati dalla Banca Nazionale di Sviluppo Polacca (BGK) per progetti di modernizzazione infrastrutturale e sicurezza informatica.
Le **super-deduzioni fiscali fino al 200%** per attività di ricerca e sviluppo (programma STEP—Strategic Technologies for Europe Platform) rappresentano un ulteriore incentivo per investimenti in innovazione tecnologica.

3. Bandi Europei di Ricerca e Innovazione. Attraverso il **programma Horizon Europe**, le aziende italiane e polacche possono accedere congiuntamente a **finanziamenti per project-based R&D in cybersecurity**.
Il **SECURE Project** (Strengthening EU SMEs Cyber Resilience), con budget totale di €22 milioni e coordinato dall'ACN, fornisce €16,5 milioni in finanziamenti a cascata direttamente agli SME europei per l'implementazione della Cyber Resilience Act nel periodo 2025-2027, offre formazione, supporto tecnico e co-finanziamento per PMI europee che implementano misure di sicurezza informatica e conformità alla Cyber Resilience Act.

4. Co-finanziamento Pubblico-Privato. Molte municipalità e istituzioni polacche hanno lanciato bandi per **partnership pubblico-privata (PPP) nel settore della sicurezza informatica**. Questi progetti offrono opportunità di revenue sharing e contratti di lungo termine, garantendo stabilità commerciale per le aziende italiane partner.

Scenario Realistico di Opportunità

Per illustrare concretamente il potenziale di mercato, consideriamo il caso di una **società energetica polacca di medie dimensioni** che opera nella distribuzione di energia elettrica in una regione centrale (ad esempio, la regione di ?ód?). Questa società è classificata come **"essential entity"** secondo NIS2, il che significa che deve implementare un **information security management system (ISMS)** conforme ai standard ISO/IEC 27001:2022 entro **sei mesi dalla promulgazione della legge di transposizione polacca** (attualmente prevista per la prima metà del 2026).

L'azienda energetica ha riconosciuto che la sua infrastruttura IT attuale, prevalentemente basata su sistemi legacy, non è sufficientemente resiliente agli attacchi cyber. **Necessita di:**

- una **valutazione del rischio di cybersicurezza** secondo il framework NIST e le linee guida ENISA;
- la **ridefinizione dell'architettura IT** per implementare defense-in-depth, multi-factor authentication, e encryption end-to-end;
- la **creazione di un Security Operations Center (SOC)** con capacità di monitoraggio 24/7 e incident response; (*d*) il **trasferimento di competenze** al team interno per garantire la sostenibilità operativa.

Una **società italiana specializzata in managed security services (MSSP) con expertise nel settore energetico** potrebbe proporre una **soluzione integrata** che combini:

- una **piattaforma SIEM/SOAR** (Security Information and Event Management / Security Orchestration, Automation and Response) fornita da partner tecnologici internazionali,
- **servizi di consulenza in governance della sicurezza**,
- **staffing di specialisti in cybersecurity** che operino nel SOC,
- **programmi di training per il team locale**,
- **supporto alla conformità NIS2** e agli audit regolamentari. Il costo totale della soluzione potrebbe ammontare a **1,5-2,5 milioni di euro su tre anni**.

L'azienda energetica polacca potrebbe finanziare questo progetto ricorrendo a: **fondi KPO** allocati direttamente alla modernizzazione della cybersicurezza infrastrutturale; **crediti bancari agevolati** della BGK; **contributi del governo locale** per la protezione infrastrutturale; **risorse interne**. Per la società italiana, questo rappresenterebbe un **contratto ancorabile** con potenziale di estensione o replicazione in altri settori e geografie polacche.

Conclusioni: Opportunità Concrete e Prossimi Passi

La convergenza tra **esigenze normative urgenti**, **finanziamenti pubblici cospicui**, **minacce cyber strutturali**, e **expertise italiana consolidata** crea un ambiente di mercato straordinariamente favorevole per le aziende italiane del settore della cybersicurezza. La **Polonia non rappresenta solamente un mercato di sbocco**, ma un partner strategico per sviluppare sinergie operativo-commerciali, ampliare la propria base di clienti europei, e rafforzare la propria competitività a livello continentale.

Fonti: Commissione Europea; Ministero degli Affari Digitali Polacco; ENISA (EU Agency for Cybersecurity); Agenzia per la Cybersicurezza Nazionale Italiana; Polish Investment and Trade Agency (PAIH)

(Contributo editoriale a cura della Camera di Commercio e dell'Industria Italiana in Polonia [2])
Ultima modifica: Martedì 27 Gennaio 2026

Condividi

Reti Sociali

ARGOMENTI

Source URL: https://www.assocamerestero.com/notizie/cybersecurity-direttiva-nis2-opportunita-strategica-aziende-italiane-nel-mercato-polacco

Collegamenti
[1] https://www.assocamerestero.com/notizie/%3Ffield_notizia_categoria_tid%3D1122
[2] https://www.assocamerestero.it/ccie/camera-commercio-dellindustria-italiana-polonia