CONFINDUSTRIA
VENETO EST
Area Metropolitana
Venezia Padova Rovigo Treviso

Appuntamenti con l'InnovAzione 2025

IA & CYBERSECURITY:
una guida per capire come l'IA può davvero rafforzare la Cybersecurity

29 settembre 2025

IL RELATORE

Lorenzo Celussi
CISO e Resp. ISO 27001

Tinet®
DIGITAL SOLUTIONS

Azienda certificata ISO 27001
CSQA
GESTIONE SICUREZZA delle INFORMAZIONI

TINET srl è un **System Integrator IT** con sede principale in provincia di Treviso: offriamo soluzioni e servizi IT evoluti, con un forte **focus sulla cybersecurity**.

CHI È TINET

TINET è una società che offre soluzioni informatiche e digitali ad aziende, professionisti ed enti pubblici, abbinando ai prodotti hardware e software un'ampia gamma di servizi.

www.tinet.it

VISION

Il Partner Tecnologico di riferimento per il pubblico ed il privato nel Nord Est

VALUE

Sostenibilità, Sicurezza ed Efficienza

MISSION

Scegliere e declinare le tecnologie per renderle semplici e produttive

DATI 2024

44	3	85	19,7
ANNI DI ATTIVITÀ	SEDI OPERATIVE	ADDETTI	FATTURATO

INTRODUZIONE

Il clamore sull'intelligenza artificiale nella cybersecurity è inarrestabile.

*L'**IA** promette **più protezione**, **meno costi** e **meno personale**,*
*ma apre anche la strada a una **nuova era di attacchi informatici***

Questa guida aiuterà le organizzazioni a orientarsi, descrivendo come l'IA può **rafforzare le difese informatiche**, **esplorando i rischi operativi** che essa stessa introduce

L'obiettivo è sempre garantire la massima resilienza informatica con costi ottimizzati.

Insight Sophos Gennaio 2025

TIPOLOGIE DI IA NELLA CYBERSECURITY

IA basata sul deep learning *Applicazione*

Utilizza reti neurali artificiali per riconoscere pattern e prendere decisioni con un processo che imita il funzionamento del cervello umano. APPLICA le informazioni apprese per svolgere attività.

Esempio: **Rilevamento degli URL malevoli**

Il modello di IA è addestrato per identificare i siti web pericolosi, permettendo così agli strumenti di sicurezza di bloccare l'accesso a questi siti

Intelligenza artificiale generativa *Creazione*

Utilizza la struttura e i pattern dei dati esistenti per CREARE (generare) nuovi contenuti.

Esempio: **Riepilogo di un caso di minaccia**

Il modello di IA crea un riepilogo dell'attività della minaccia e fornisce agli analisti un elenco di azioni successive consigliate

*Whitepaper Sophos Gennaio 2025

VANTAGGI DELL'IA NELLA CYBERSEC

Migliore protezione contro le minacce informatiche (20%)
Maggiore ritorno sull'investimento nella cybersecurity (20%)
Maggiore impatto ed efficienza per gli analisti informatici (17%)
La certezza di tenere il passo con le innovazioni della cybersecurity (15%)
Maggiore tranquillità nel sapere che la nostra organizzazione è adeguatamente protetta contro gli attacchi (14%)
Minore rischio di burnout per i dipendenti, automatizzando le attività per concedere più tempo ai dipendenti che si occupano della cybersecurity (14%)

*Whitepaper Sophos Gennaio 2025

TASSO DI ADOZIONE DELL'IA NELLA CYBERSEC

73%
Usa strumenti di cybersecurity con modelli di deep learning

65%
Usa strumenti di cybersecurity con funzionalità GenAI

99%
Richiede funzionalità di IA quando deve scegliere una piattaforma di cybersecurity

Con questi tassi di adozione e utilizzo futuro, **comprendere** quali sono **i rischi dell'IA nella cybersecurity** e come **mitigarli** è una delle **priorità principali** per le organizzazioni di qualsiasi dimensione e ambito operativo.

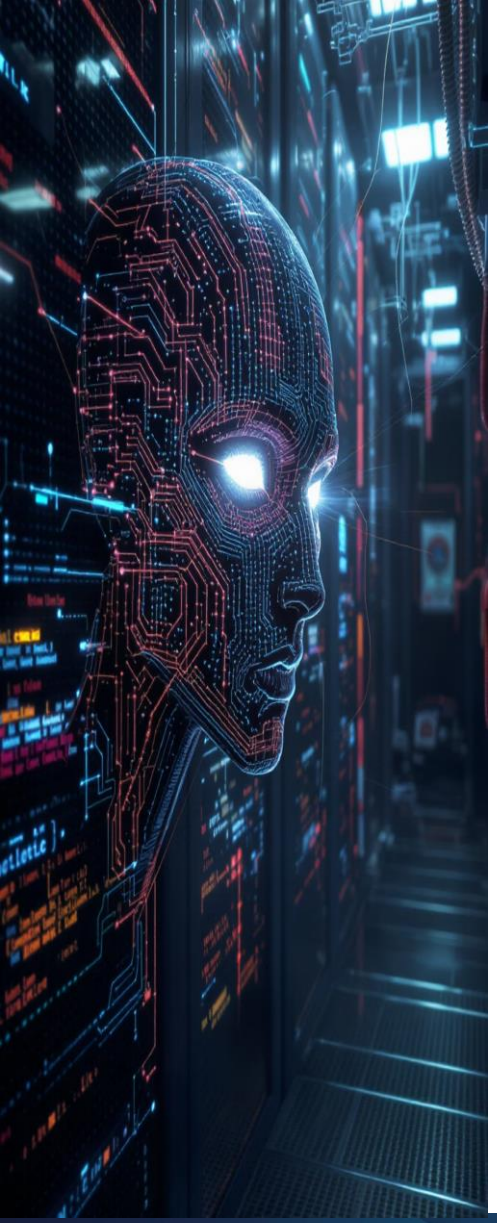
*Whitepaper Sophos Gennaio 2025

LE LIMITAZIONI DELL'INTELLIGENZA ARTIFICIALE

L'IA completa le capacità umane, ma non le rimpiazza

Affidarsi esclusivamente all'intelligenza artificiale non è la risposta.

⚠ Da sola, l'IA non è in grado di anticipare le abili organizzazioni cybercriminali del giorno d'oggi.



I RISCHI DELL'IA NELLA CYBERSECURITY

L'uso dell'IA nella cybersecurity è una spada a **doppio taglio**.
Offre **enormi vantaggi** ma introduce **anche diversi rischi**:

Rischio in termini di minacce

Rischio in termini di difese

Rischio operativo

Rischio finanziario

Rischio di sabotaggio

RISCHIO IN TERMINI DI MINACCE

I cybercriminali sfruttano l'IA principalmente per migliorare qualità dei contenuti e rilevare nuove vulnerabilità.

Migliorare la qualità dei contenuti

Elevare qualità e credibilità delle e-mail di phishing eliminando errori grammaticali e di battitura con LLM pubblici.

Clonazione vocale

Tecnologie avanzate per **convincere vittime fingendosi dirigenti aziendali** in attacchi di **vishing**.

Video deepfake

Imitazione visiva per **indurre dipendenti a trasferire denaro** e ingannare programmi di riconoscimento facciale.

RISCHIO IN TERMINI DI DIFESE

L’implementazione inadeguata di **modelli di IA di scarsa qualità** può introdurre **gravi rischi di sicurezza**. Ciò dipende da vari fattori:

Qualità dei dati di apprendimento

Dati sbagliati producono risultati sbagliati. Questo può portare a una rappresentazione distorta delle minacce, con falsi positivi o negativi.

Competenze tecniche dei team

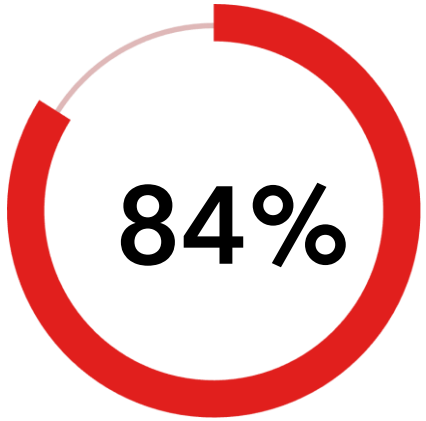
È fondamentale che i team preposti alla difesa informatica abbiano competenze sia in Cybersecurity che in IA

Qualità del processo di sviluppo

Senza adeguati processi di test e implementazione, l'IA può causare danni gravi e difficili da identificare.

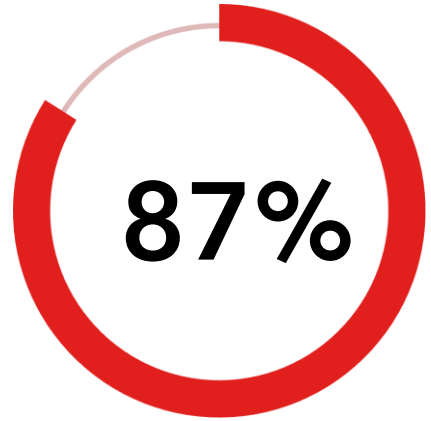
RISCHIO OPERATIVO

L'IA, ormai, influisce su quasi tutti gli aspetti delle nostre vite quotidiane, rendendo fin troppo facile ricorrere automaticamente all'IA per qualsiasi cosa – **Eccessiva fiducia nell'IA** può **portare a negligenza umana** e a **una riduzione della supervisione critica**



Preoccupazioni riduzione personale

Nutre preoccupazioni sulle pressioni di ridurre il personale esperto



Mancanza di responsabilità

Nutre preoccupazioni sulla conseguente mancanza di responsabilità

RISCHIO FINANZIARIO E DI SABOTAGGIO

L'integrazione dell'IA, in particolare della GenAI, presenta una duplice sfida: i **costi significativi di sviluppo e gestione**, e la **crescente vulnerabilità ad attacchi mirati**. La gestione efficace di questi aspetti è cruciale per la sicurezza e la redditività aziendale.

Rischio Finanziario

Il **75%** degli IT Manager sostiene che **i costi dell'IA sono difficili da misurare** accuratamente, mettendo **a rischio il ritorno sull'investimento** senza una reportistica efficace.

Rischio di Sabotaggio

L'adozione diffusa dell'IA aumenta il rischio di attacchi malevoli esterni ed interni. **Il sabotaggio può manifestarsi** tramite l'**alterazione dei dati di addestramento** (data poisoning), la **manipolazione dei modelli** per indurre errori o comportamenti indesiderati, o l'**interruzione dei sistemi IA critici**.

PROTEZIONE DELLA PROPRIETÀ INTELLETTUALE E DEI DATI RISERVATI

🔐 Le informazioni riservate come brevetti, strategie e know-how sono asset critici per ogni impresa.

⚠️ **L'uso dell'IA può esporre questi dati a rischi**:

- Data leakage involontario
- Memorizzazione nei modelli IA
- Attacchi mirati a infrastrutture IA

🛡️ **Misure di protezione**:

- *Analizzare le policy dei modelli IA sulla gestione dei dati inseriti*
- Uso consapevole dell'IA
- Formazione del personale
- Definire una politica aziendale chiara sull'utilizzo dell'IA

👔 Valutare attentamente l'utilizzo dei modelli IA, in quanto proteggere la proprietà intellettuale significa proteggere il valore della propria azienda.

CONSIGLI PRATICI PER ORIENTARSI NEL CLAMORE

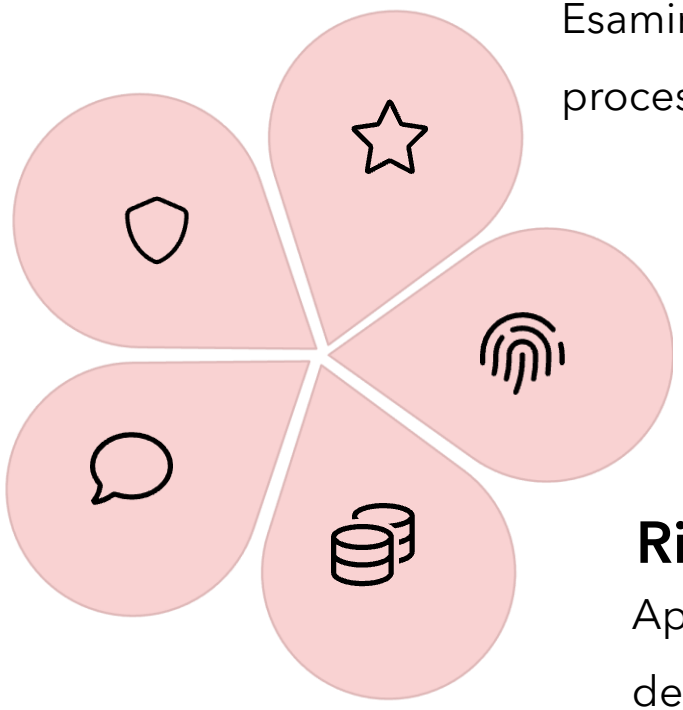
Adottando un approccio ponderato, le organizzazioni possono orientarsi meglio e **sfruttare in maniera sicura** i **vantaggi dell'IA** per potenziare le proprie difese informatiche.

Migliorare le Difese Informatiche

Rafforzare la protezione contro le minacce cibernetiche, con un focus su email, attacchi BEC, Social Media e Anti Clonazione Vocale.

Consapevolezza dei Rischi

Mantenere un'alta consapevolezza riguardo al potenziale sabotaggio e vulnerabilità dell'IA.



Valutare la Qualità dell'IA

Esaminare attentamente i dati, i team e i processi di sviluppo dei modelli AI.

Prospettiva Umana

Considera l'AI solo uno strumento che ha vantaggi nell'automazione ma non sostituta delle tue risorse umane.

Rigore Aziendale

Applicare lo stesso rigore analitico alle decisioni di investimento tradizionali nell'IA: obiettivi – bisogni – vantaggi – priorità - impatto

CONCLUSIONE

L'IA offre enormi vantaggi per la cybersecurity

Adottando un approccio ponderato e focalizzato sui risultati, le organizzazioni possono **sfruttare l'IA per rafforzare le proprie difese informatiche**. L'obiettivo è potenziare gli esperti IT e di cybersecurity, **mantenendo sempre la responsabilità umana al centro delle decisioni strategiche**.

Con il giusto approccio, l'IA diventa un alleato potente nella lotta contro le minacce informatiche.

Per informazioni:
ricercainnovazione@confindustriavenest.it

Grazie per l’attenzione.