Tech*Trend*

10
Ai
Artificial
Intelligence

AI e Cybersecurity:
innovazione nella sicurezza
delle imprese

TeamSystem

TechTrend

L’obiettivo di questo documento è comprendere il ruolo dell’Intelligenza Artificiale nella Cybersecurity, analizzando le sue applicazioni nella protezione dei dati e nella prevenzione degli attacchi informatici che colpiscono le imprese, indipendentemente dalla loro dimensione. Attraverso esempi concreti e case study, il lettore scoprirà l’efficacia dell’AI nella prevenzione di attacchi e nella gestione delle emergenze legate alla sicurezza informatica.

Indice

AI e Cybersecurity:

innovazione nella sicurezza delle imprese

Negli ultimi anni, l'**accelerazione dell'innovazione digitale** ha prodotto una profonda trasformazione del mondo delle imprese, portando a un notevole incremento di efficienza, produttività e competitività. Una crescita esponenziale che ha avuto però un effetto collaterale: l'**aumento delle minacce informatiche**.

AI e Cybersecurity: innovazione nella sicurezza delle imprese

Chi fa impresa oggi ha imparato a familiarizzare con termini che, in passato, erano appannaggio esclusivo degli esperti di informatica, tanto che non ci si limita più a riferirsi genericamente a "**virus**" o "**malware**": **attacchi ransomware**, **phishing**, **furto di credenziali** e **violazioni dei dati** sono diventate espressioni di uso comune e rappresentano minacce sempre più frequenti e sofisticate, che mettono a rischio le aziende di tutte le dimensioni. Se in passato la **Cybersecurity** era considerata un'attività di nicchia o competenza del solo reparto IT, oggi deve essere quindi una **priorità strategica** per qualsiasi organizzazione, dalle grandi multinazionali alle piccole e medie imprese.

Gli attacchi cyber, infatti, non solo compromettono dati sensibili e operatività aziendale, ma possono anche danneggiare la reputazione dell'impresa e causare ingenti perdite economiche.

In questo scenario complesso, **l'Intelligenza Artificiale (AI) si sta affermando come un'alleata fondamentale nella protezione delle infrastrutture digitali**. Grazie alla sua capacità di analizzare grandi volumi di dati in tempo reale, riconoscere anomalie e rispondere in modo tempestivo alle minacce, l'AI sta trasformando il modo in cui le aziende affrontano la Cybersecurity.

L'Intelligenza Artificiale offre tre vantaggi principali alla sicurezza informatica delle imprese:

protezione, grazie a strumenti di monitoraggio e rilevamento delle minacce basati su algoritmi di Machine Learning;

prevenzione degli attacchi informatici attraverso l'analisi predittiva, che identifica le vulnerabilità nei sistemi aziendali e interviene prima che queste vengano sfruttate dagli hacker;

resilienza, ossia la capacità di rispondere tempestivamente e riprendersi rapidamente da un attacco informatico.

In questo documento, esploreremo nel dettaglio l'**evoluzione della Cybersecurity attraverso l'AI**, le principali tipologie di attacchi cyber e le strategie più efficaci da attuare per difendersi in modo efficace. Dopo aver analizzato l'impatto dell'Intelligenza Artificiale sulla sicurezza aziendale esamineremo le prospettive future del settore, offrendo uno sguardo d'insieme sul modo in cui le imprese possono sfruttare al meglio le nuove tecnologie per **proteggere il proprio business in un mondo sempre più digitale e interconnesso**.

Per saperne di più:

→ AI svelata: una guida pratica all'intelligenza artificiale, per tutti

→ AI o Intelligenza Artificiale

→ Cybersecurity: cos'è e perché è fondamentale per ogni impresa

→ Cybersecurity: proteggi la tua impresa con la guida completa di TeamSystem

→ Investimenti PNRR nella Cybersecurity per rafforzare le difese di aziende e PA

Capitolo 1

Il Fintech e il nuovo paradigma della gestione finanziaria nelle PMI

La sicurezza informatica è una catena fatta di molti anelli: ognuno va valutato con attenzione, perché la solidità dell'intero sistema dipende dalla capacità di individuare e rinforzare proprio l'anello più debole. Storicamente questo modello è stato fondato su approcci reattivi, che hanno vissuto una profonda trasformazione grazie all'introduzione dell'Intelligenza Artificiale. Se in passato si interveniva solo dopo che un attacco era stato identificato, appunto per rinforzare l'anello più debole, oggi l'**AI consente un cambio di paradigma**: un **approccio proattivo**, capace non solo di prevenire le minacce, ma anche di rispondere in modo automatizzato agli incidenti, migliorando sensibilmente la resilienza operativa delle aziende. Facciamo un esempio: in caso di rilevamento di una minaccia, i sistemi basati sull'AI possono attivare in automatico misure difensive, come l'isolamento di una macchina o di un software compromessi, la revoca temporanea delle credenziali o il blocco di un indirizzo IP sospetto. Questa rapidità di reazione è essenziale per limitare i danni e assicurare la continuità operativa.

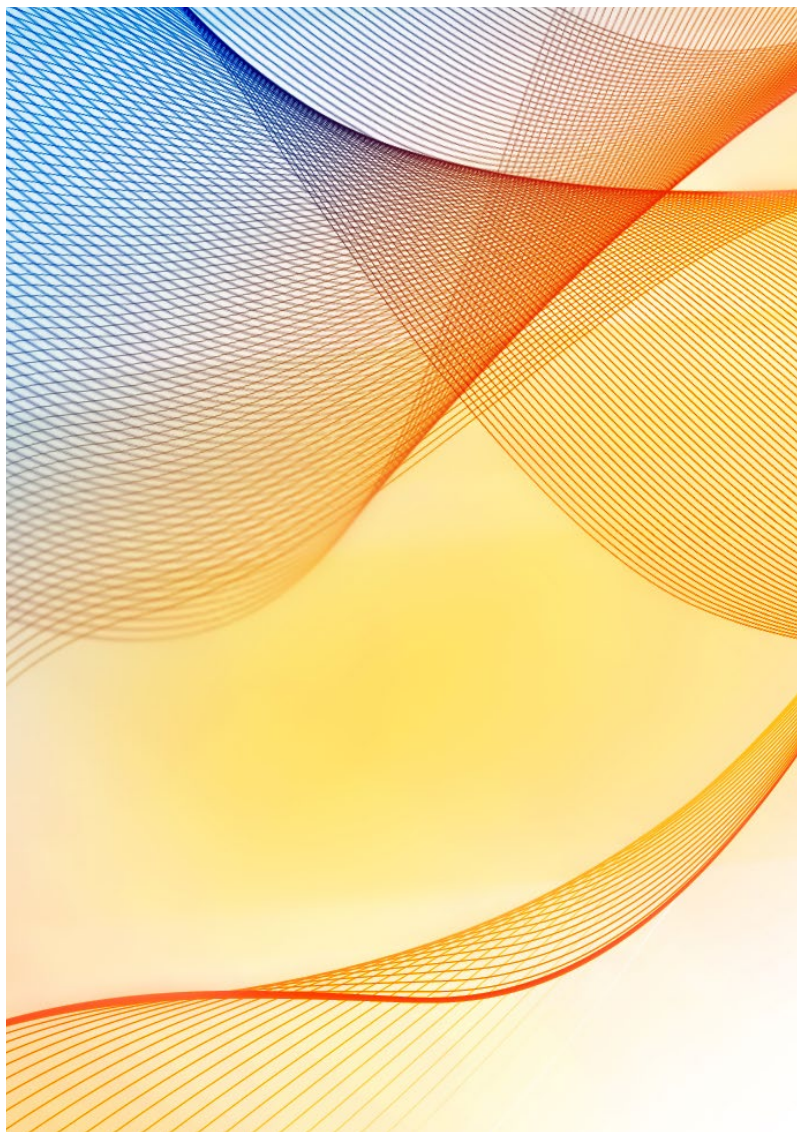
Altro aspetto importante di un sistema che sfrutta l'Intelligenza Artificiale per la sicurezza informatica risiede nella sua **capacità di analizzare grandi quantità di dati**, e di identificare più velocemente anomalie che potrebbero rappresentare una minaccia imminente. Ad esempio, se si registra l'accesso a file sensibili in orari insoliti o da dispositivi non autorizzati, un sistema basato sull'AI può rilevare questa attività come sospetta e segnalarla immediatamente: questo monitoraggio continuo consente alle aziende di anticipare potenziali attacchi prima che possano causare danni significativi.

Gli aspetti appena visti rappresentano un **grandissimo vantaggio per le piccole e medie imprese**, spesso sprovviste di personale dedicato alla sicurezza informatica disponibile 24 ore su 24: l'automazione offerta dall'AI, infatti, garantisce una protezione costante, una maggiore efficienza nel caso di intervento a un attacco e una maggiore stabilità di tutti i sistemi aziendali.

Implementando queste soluzioni, le aziende possono ridurre il tempo di risposta agli incidenti e minimizzare l'impatto di potenziali attacchi. Lo confermano anche i dati. Secondo uno **studio del Ponemon Institute**, il **66% delle aziende utilizza l'AI per rilevare attacchi in ambienti Cloud**, on-premises (ovvero infrastrutture IT e sistemi informatici installati e gestiti direttamente all'interno dell'azienda, nei suoi data center o server locali) e ibridi, e il 70% ritiene che l'AI sia altamente efficace nell'individuare minacce precedentemente non rilevabili. Inoltre, il 51% degli alert di sicurezza può essere gestito in automatico dall'Intelligenza Artificiale, riducendo così il carico di lavoro umano.

Ma ripercorriamo nel dettaglio come la sicurezza informatica si è evoluta grazie all'applicazione dell'Intelligenza Artificiale.

1.1 L'evoluzione della sicurezza con l'AI



Per comprendere il contesto in cui le aziende sono chiamate a rafforzare le proprie difese digitali, è essenziale considerare la natura sempre più sofisticata delle minacce informatiche. Ogni attacco nasce da un antagonismo tra chi tenta di violare i sistemi e chi è incaricato di proteggerli. Gli attori malevoli sfruttano vulnerabilità tecniche e organizzative per accedere alle infrastrutture aziendali, mentre i responsabili della sicurezza devono anticipare le mosse degli aggressori, implementando soluzioni di difesa proattive e aggiornate. Con l'avvento dell'Intelligenza Artificiale, sia gli strumenti offensivi che quelli difensivi stanno rapidamente evolvendo, rendendo il panorama ancora più complesso e dinamico.

Comprendere come "ragioni" l'avversario è la prima regola per predisporre difese adeguate e cogliere i vantaggi delle nuove tecnologie. Se un tempo la sicurezza era basata su approcci statici, come firewall e antivirus con firme predefinite, oggi **l'Intelligenza Artificiale consente una difesa dinamica e adattiva**. Grazie alla capacità di apprendere dai dati e di riconoscere schemi sospetti, i sistemi di Cybersecurity basati sull'AI non si limitano a bloccare minacce già note, ma riescono a identificare e contrastare anche attacchi mai visti prima.

Un esempio concreto di questa trasformazione è l'**utilizzo del Machine Learning** per il rilevamento delle minacce: gli algoritmi analizzano in tempo reale il traffico di rete e il comportamento degli utenti, individuando anomalie che potrebbero indicare attività malevole. Il Machine Learning, quindi, si rivela particolarmente **efficace nel riconoscere violazioni dei dati e identificare accessi non autorizzati**: questo significa, ad esempio, che un accesso insolito a un server aziendale o un volume anomalo di trasferimento dati possono essere immediatamente segnalati come potenziali indicatori di compromissione, consentendo interventi tempestivi prima che un attacco si concretizzi.

Ma non solo. Un'altra caratteristica fondamentale del Machine Learning è la capacità di correlare informazioni provenienti da diverse fonti, come il traffico di rete, i log di accesso e le e-mail ricevute, per identificare pattern sospetti. Questo approccio permette di migliorare la **capacità di individuare attacchi "zero-day"**, cioè minacce nuove per cui non esistono ancora firme di sicurezza specifiche. Inoltre, il Machine Learning riduce il numero di falsi positivi, **filtrando gli alert realmente critici** e assottigliando il carico di lavoro degli analisti di sicurezza. Grazie alla sua capacità di adattarsi costantemente all'evoluzione delle minacce, dunque, il Machine Learning offre alle aziende un vantaggio strategico, migliorando la velocità di risposta e ottimizzando l'allocazione delle risorse per la sicurezza informatica.

Servendosi di queste innovazioni, l'Intelligenza Artificiale sta rendendo la sicurezza informatica molto più efficace e proattiva, e fornisce alle aziende uno strumento di difesa prezioso per far fronte a minacce sempre più complesse.

1.2 Tecnologie AI-driven per la Cybersecurity

Come abbiamo visto, le tecnologie che sfruttano l'Intelligenza Artificiale rappresentano oggi uno strumento strategico per rafforzare la sicurezza informatica. Grazie alla loro capacità di analizzare enormi volumi di dati in tempo reale, questi sistemi sono in grado di rilevare comportamenti anomali o segnali di minacce che potrebbero sfuggire ai controlli tradizionali, permettendo una risposta più tempestiva e precisa agli attacchi.

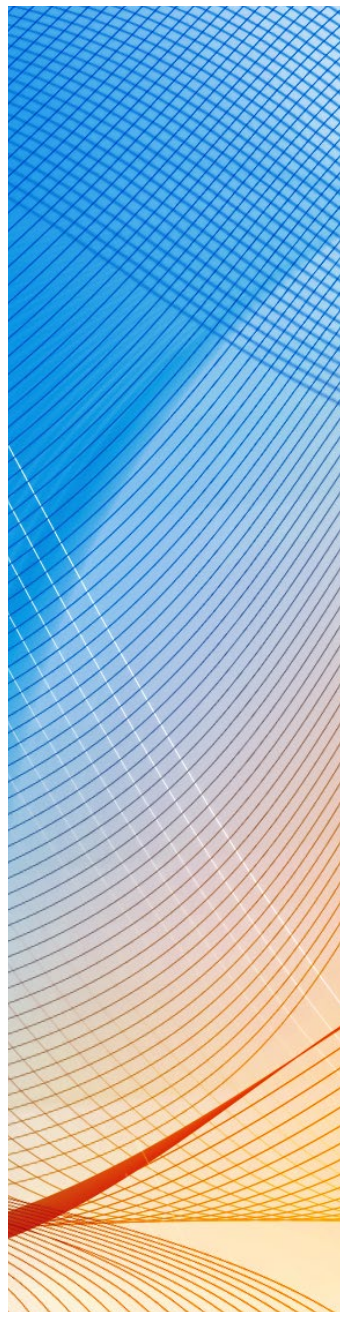
Un esempio emblematico di queste minacce emergenti e nascoste è rappresentato dal **deepfake**, una **tecnica che sfrutta l'Intelligenza Artificiale per creare contenuti video o audio falsificati** in maniera estremamente realistica. I deepfake vengono utilizzati per manipolare video e registrazioni vocali, facendoli sembrare autentici, con l'obiettivo di truffare, diffondere disinformazione, danneggiare reputazioni o compromettere la sicurezza aziendale. Questi attacchi, difficili da rilevare senza un'analisi avanzata, rappresentano una nuova frontiera nella battaglia informatica, minacciando non solo la privacy, ma anche l'integrità delle comunicazioni e delle transazioni.

Ad esempio, un tentativo di truffa ai danni di **Ferrari** ha coinvolto l'uso di deepfake per imitare la voce del CEO Benedetto Vigna e convincere un dirigente a trasferire fondi per un'acquisizione fittizia: i truffatori hanno inviato messaggi WhatsApp da un numero sconosciuto, preceduti da una telefonata in cui la voce sembrava autentica. Tuttavia, grazie a una domanda personale posta dal dirigente, l'inganno è stato scoperto e Ferrari ha avviato un'indagine per evitare danni economici e reputazionali. Questo episodio mette in luce **l'importanza di procedure di verifica** per prevenire simili attacchi e suona come un campanello d'allarme per le piccole e medie imprese, che al pari di un colosso come Ferrari, rischiano quotidianamente di diventare oggetto di aggressioni di questo tipo.

L'AI ha rivoluzionato anche la ***threat intelligence***, ossia **la raccolta e l'analisi dei dati relativi alla cronologia delle minacce per bloccare e correggere gli attacchi informatici** prima che si verifichino. Grazie alla sua capacità di analizzare dati come il traffico di rete, le comunicazioni interne e i pattern di accesso ai sistemi, l'AI è in grado di rilevare segnali anche minimi che potrebbero indicare vulnerabilità. Questi segnali, come comportamenti insoliti degli utenti o un incremento improvviso di attività su un determinato sistema, possono passare inosservati agli occhi umani, ma per i sistemi basati sull'AI sono precursori di minacce potenziali. Inoltre, l'Intelligenza Artificiale è in grado di adattarsi alle nuove informazioni, aggiornando di continuo i modelli di rilevamento per migliorare la capacità di identificare e rispondere alle minacce emergenti: questo **processo di continuo auto-apprendimento** rende le difese aziendali sempre più robuste e dinamiche, con un miglioramento continuo delle capacità predittive.

Infine, la sicurezza informatica basata su tecnologie **Cloud** gioca un ruolo cruciale. Le **soluzioni di Cybersecurity basate sul Cloud**, infatti, consentono alle aziende di mantenere i propri **sistemi di difesa sempre aggiornati**, senza la necessità di gestire manualmente gli update, e sono progettate per adattarsi velocemente alle nuove minacce e garantire una protezione sempre all'avanguardia.

Nei capitoli successivi, esploreremo le principali tipologie di attacchi informatici e le strategie di difesa più efficaci, con particolare attenzione a come l'Intelligenza Artificiale possa essere utilizzata per contrastare minacce come il phishing, il malware e i deepfake.



Per saperne di più:

→ Sicurezza informatica aziendale: la situazione nelle imprese italiane

→ Come prevenire la fuga dei dati aziendali e proteggere la tua azienda

→ Cybersecurity: i costi delle violazioni informatiche nelle aziende

Approfondimento

Dati e numeri sulle minacce informatiche

Le minacce informatiche continuano a crescere con un ritmo costante e che desta preoccupazione. Nel 2024, come esaminato dal **report Clusit**, sono stati rilevati 3.541 incidenti a livello globale, con un incremento del 27,4% rispetto all'anno precedente. Questo segna una crescente sofisticazione e diffusione dei cyber attacchi, che stanno mettendo a dura prova la sicurezza delle organizzazioni in tutto il mondo.

Impatto in Italia:

- **il 78% degli attacchi in Italia nel 2024 è stato attribuito al cybercrime**, evidenziando la preoccupante diffusione di attacchi motivati da guadagni economici illeciti;
- **l'Italia ha subito il 10% degli attacchi globali**, un dato che sottolinea quanto il nostro Paese sia interessante per i criminali informatici;
- **news e multimedia sono le categorie più colpite**, con il 18% degli attacchi totali. Altri settori vulnerabili includono il manifatturiero e il trasporto e logistica, che rappresentano un quarto degli incidenti a livello mondiale.

Principali minacce:

- **malware**: è la minaccia più diffusa, riguardando il 32% degli incidenti conosciuti. Tra questi, il ransomware è il tipo di malware più utilizzato, responsabile dell'81% degli attacchi malware globali;
- **phishing e ingegneria sociale**: sono cresciuti del 33% rispetto al 2023, con un aumento particolarmente significativo in Europa (+67%) negli incidenti di maggiore impatto;
- **sfruttamento di vulnerabilità (zero-day)**: ha rappresentato il 15% degli attacchi globali.

Dati sull'impatto degli attacchi:

- **il 79% degli attacchi globali nel 2024 ha avuto un impatto grave o critico**, con conseguenze per aziende, enti pubblici e cittadini;
- gli **attacchi DDoS** ad alta banda (ovvero in cui un grande numero di dispositivi, spesso compromessi e controllati da hacker, viene utilizzato per inviare un volume massiccio di traffico verso un server o una rete specifica) sono aumentati del 300% rispetto all'anno precedente, indicando un'escalation della potenza e della frequenza di queste aggressioni.

Capitolo 2

Le principali tipologie di attacchi cyber e come difendersi

In un panorama sempre più complesso, **l'Intelligenza Artificiale può essere vista come uno strumento a doppio uso:** se da un lato, infatti, è utilizzata dai criminali informatici per perfezionare gli attacchi e superare le difese tradizionali, dall'altro rappresenta un alleato potente per i sistemi di Cybersecurity, che la impiegano per analizzare dati, rilevare attività sospette e prevenire minacce in tempo reale.

Come abbiamo avuto modo di osservare in precedenza, l'AI permette, infatti, di identificare schemi anomali e potenziali minacce con una velocità e un'accuratezza che superano le capacità umane. Questo la rende uno strumento essenziale per rafforzare le difese informatiche, **anticipando e neutralizzando gli attacchi** prima che possano causare danni gravi. Nonostante il potenziale uso malevole, quindi, è importante sottolineare come **le applicazioni difensive dell'AI superino di gran lunga quelle offensive.**

Secondo il 2025 Global Threat Report di **CrowdStrike**, le **piccole e medie imprese sono tra le principali vittime di attacchi informatici.** Il dato più preoccupante riguarda il fatto che **il 52% degli attacchi è legato alla fase di accesso iniziale**, momento in cui i cybercriminali penetrano nei sistemi aziendali sfruttando vulnerabilità non presidiate. Ciò significa che le aziende devono porre **grande attenzione alla difesa dei punti di ingresso della rete**, per evitare che gli hacker possano sfruttarne le lacune. Inoltre, **il 79% di questo tipo di attacchi avviene senza l'uso di malware**, ma sfruttando credenziali compromesse, permettendo quindi agli aggressori di infiltrarsi nei sistemi fingendosi utenti legittimi. A completare questo quadro, il report segnala una crescita del 73% negli attacchi mirati, come il ransomware, con impatti devastanti per le aziende colpite. L'insieme di queste informazioni evidenzia come gli aggressori stiano adottando tecniche sempre più sofisticate, che rende necessario per le aziende implementare strategie di difesa altrettanto all'avanguardia.

Esploriamo quindi le diverse tipologie di attacchi cui le aziende devono far fronte e vediamo come l'Intelligenza Artificiale può supportarle durante le fasi critiche.

2.1 Le minacce informatiche più diffuse per le imprese

Gli attacchi informatici rappresentano una minaccia sempre più concreta e pervasiva per le aziende, che riguarda non solo la sicurezza dei dati, ma anche la continuità operativa e la fiducia del mercato. Le tecniche utilizzate dai cybercriminali evolvono rapidamente, sfruttando vulnerabilità tecniche, errori umani e sofisticate manipolazioni psicologiche.

Secondo il Rapporto OAD 2024 di AIPSI, il **72,4% delle aziende italiane** ha subito almeno un attacco informatico nell'ultimo anno, confermando quanto la cybersecurity sia oggi una priorità trasversale per tutte le organizzazioni, indipendentemente dalla dimensione o dal settore.

Tra le minacce più diffuse emergono:

- la **manomissione di software e configurazioni di sistema** (31,7%), spesso invisibile fino all'attivazione dell'attacco;
- gli **attacchi DoS/DDoS** (20,7%), che puntano a bloccare servizi e infrastrutture digitali attraverso il sovraccarico dei server;
- l'**uso improprio delle risorse aziendali** (18,3%), come la sottrazione di potenza di calcolo per fini illeciti (es. cryptojacking);
- gli attacchi alla **supply chain** (15%), un trend in crescita che punta a colpire fornitori o partner per penetrare indirettamente nei sistemi aziendali.

Dal punto di vista delle **tecniche adottate**, i criminali informatici prediligono approcci sempre più articolati:

- attacchi **multi-vettore** (40,4%) che combinano exploit tecnici, malware e phishing, che è una delle tecniche più temute dalle PMI italiane, per aumentare l'efficacia offensiva;
- operazioni di **social engineering** (37,6%), capaci di aggirare i controlli sfruttando la fiducia e l'impreparazione degli utenti;
- il rilascio di **ransomware o codici malevoli** (25,3%), spesso usati per estorcere denaro o sabotare processi critici.

Un caso emblematico è quello che ha coinvolto **Trenitalia** nel 2023. Il sito web e i sistemi di prenotazione dell'azienda sono rimasti **inaccessibili per diverse ore** a causa di un attacco **DDoS (Distributed Denial of Service)** rivendicato da un gruppo di hacktivisti. Sebbene non vi sia stata una violazione dei dati o un furto di informazioni sensibili, l'attacco ha avuto **ripercussioni significative sul servizio agli utenti**, con blocchi nella vendita dei biglietti e disagi generalizzati per i viaggiatori.

Questo episodio dimostra come, anche in assenza di una compromissione diretta dei dati, **un'interruzione dell'operatività digitale possa generare danni reputazionali e impatti economici per un'azienda**. In contesti ad alta interazione con il pubblico, come quello dei trasporti, l'affidabilità dei sistemi digitali è cruciale quanto la loro sicurezza. Per questo motivo, la capacità di **prevenire e mitigare attacchi DDoS tramite strumenti di rilevamento avanzato e tecnologie AI** è diventata una priorità anche per le imprese di medie dimensioni, che sempre più spesso si trovano esposte a minacce analoghe.

In uno scenario così complesso, l'utilizzo di soluzioni basate su **Intelligenza Artificiale** diventa cruciale: solo tecnologie in grado di analizzare grandi volumi di dati in tempo reale, riconoscere pattern sospetti e attivare risposte automatiche possono, infatti, garantire un livello di protezione adeguato alle minacce odierne.

2.2 L'AI come scudo contro gli attacchi informatici

In questo scenario, l'Intelligenza Artificiale giunge in soccorso delle aziende. Anziché limitarsi a rispondere agli attacchi dopo che si sono verificati, infatti, l'AI gioca un ruolo determinante nell'**anticipare le minacce**, monitorare i sistemi aziendali e rafforzare i meccanismi di accesso.

Attraverso **modelli di apprendimento automatico** e **algoritmi avanzati**, l'AI è in grado di **analizzare grandi quantità di dati storici**, rilevando pattern ricorrenti o segnali deboli associabili a minacce note. Ma il suo vero punto di forza è la capacità di **generalizzare da eventi passati per riconoscere comportamenti sospetti anche in contesti completamente nuovi**, non ancora codificati dalle firme degli attacchi noti.

Ricordando sempre che la protezione non si ottiene guardando solo l'insieme, ma esaminando ogni singolo elemento della catena, intervenendo per potenziare l'anello più debole.

Le tecnologie basate sull'AI possono agire concretamente come scudo contro i cyber attacchi in più modi.

Difesa predittiva: una delle capacità più importanti dell'Intelligenza Artificiale è quella di individuare le minacce prima che queste si manifestino, adattandosi dinamicamente alle nuove tattiche degli hacker. Le soluzioni predittive basate su AI si servono di tecniche in grado di individuare vulnerabilità o schemi anomali, come modifiche nei comportamenti degli utenti o del traffico di rete, per segnalare attività pericolose. L'intervento in anticipo permette di bloccare i cyber attacchi prima che causino danni significativi.

Monitoraggio e rilevamento automatico: reattività e proattività sono i tratti distintivi dei sistemi di monitoraggio basati sull'Intelligenza Artificiale, che riescono a identificare pattern anomali e rispondere automaticamente isolando la minaccia senza necessità dell'intervento umano. Grazie alla sua capacità di operare 24 ore su 24, 7 giorni su 7, l'AI garantisce una protezione continua, proteggendo l'infrastruttura aziendale da attacchi che potrebbero passare inosservati ai metodi di contrasto tradizionali, basati su regole predefinite e su firme specifiche di attacchi già noti.

Minaccia	Definizione	Contromisura AI-based
Phishing	Tentativi di inganno via e-mail o sistemi di messaggistica per ottenere dati sensibili o installare malware	• Filtri antiphishing basati su AI • Analisi semantica dei messaggi • Sistemi di scanning predittivo
Furto credenziali Accessi illeciti	Uso fraudolento di credenziali per accedere a sistemi aziendali	• Analisi comportamentale • Autenticazione adattiva AI • Rilevamento accessi anomali e segnali deboli
Ransomware e malware avanzato	Software malevolo che cripta dati o compromette i sistemi in cambio di riscatto	• Rilevamento anomalie nei file/processi • Segmentazione automatica della rete • Risposta autonoma AI
Attacchi zero-day	Sfruttamento di vulnerabilità non ancora note o corrette	• Machine Learning per riconoscere comportamenti anomali • Threat intelligence dinamica • Risposta comportamentale AI

La protezione delle reti aziendali passa, quindi, per l'implementazione di soluzioni multilivello e integrate. Le piccole e medie imprese italiane devono necessariamente **agire con rapidità, adottando soluzioni che integrano al loro interno modelli di Intelligenza Artificiale per rafforzare la sicurezza** e contrastare attacchi sempre più complessi. Nel capitolo successivo indagheremo da vicino le best practice per proteggere i dati aziendali mitigando i rischi derivanti dagli attacchi cyber.

Per saperne di più:

→ I principali tipi di attacchi informatici e come prevenirli

→ Cybersecurity: i 4 attacchi informatici più comuni in un e-commerce

→ Attacchi hacker in Italia: come le PMI possono proteggersi

Approfondimento

Le principali minacce informatiche per le aziende

- **Malware:** un software malevolo in grado di creare danni o disturbi a un programma, a un dispositivo o a una rete. I programmi malevoli non si limitano più a infettare un dispositivo, ma si modificano autonomamente per eludere gli antivirus tradizionali. Alcuni sono progettati per rimanere dormienti a lungo prima di attivarsi, mentre altri mutano continuamente il proprio codice per sfuggire al rilevamento. Un celebre caso di un recente attacco malware a una PMI è quello subito da KNP Logistics Group, un'azienda britannica con oltre 150 anni di storia alle spalle: nel giugno 2023, il gruppo ransomware Akira ha compromesso i sistemi di KNP attraverso una password debole, richiedendo un riscatto in criptovaluta e minacciando di pubblicare dati sensibili. Nonostante gli sforzi per mitigare l'attacco, l'azienda ha subito perdite di dati finanziari cruciali, cha ha compromesso la sua capacità di ottenere credito e portato alla cessazione delle attività nel giro di appena tre mesi.

- **Deepfake e social engineering avanzato:** grazie alle moderne tecnologie di manipolazione audio e video, questa tecnica permette di realizzare contenuti falsi ma incredibilmente realistici. I cybercriminali possono, ad esempio, simulare la voce di un dirigente aziendale per impartire ordini fraudolenti o falsificare videoconferenze per ingannare dipendenti e fornitori. Un rapporto di VikingCloud ha evidenziato che un terzo delle PMI ha subito un attacco informatico nell'ultimo anno, con un aumento significativo di truffe basate su deepfake, tra cui email di phishing e account falsi sui social media.

- **Ransomware:** è un particolare tipo di malware progettato per bloccare i file e i sistemi aziendali, rendendoli inutilizzabili finché non viene pagato un riscatto. Negli ultimi anni, le tecniche si sono evolute: oggi i criminali minacciano anche di divulgare dati sensibili sottratti all'azienda, aumentando la pressione per il pagamento. Un caso eclatante in Italia è quello subito dal gruppo manifatturiero Alf DaFrè, specializzato nella produzione di mobili. Nei primi mesi del 2024 l'azienda è stata colpita da un attacco informatico che ha paralizzato la produzione, causando interruzioni significative nelle operazioni e costringendo l'azienda a richiedere l'attivazione della cassa integrazione per oltre 300 dipendenti.

- **Phishing:** è una delle tecniche di attacco più semplici e allo stesso tempo efficaci. I truffatori inviano e-mail, SMS o messaggi Whatsapp spacciandosi per enti affidabili (banche, fornitori, dirigenti interni) per spingere le vittime a fornire credenziali, dati finanziari o scaricare malware. Recentemente, diverse piccole e medie imprese (PMI) italiane sono state vittime di attacchi di phishing. Secondo un rapporto dell'Osservatorio ASUS Business, quasi il 50% delle PMI ha subito almeno un attacco informatico negli ultimi tre anni, con il 51% dei dipendenti che non riesce a riconoscere una email di phishing, aumentando così il rischio di compromissione dei dati aziendali.

- **Violazioni di dati e furti di credenziali:** i criminali sfruttano vulnerabilità nei sistemi aziendali per accedere illegalmente a database e rubare informazioni sensibili. Le credenziali sottratte possono essere vendute nel dark web o utilizzate per attacchi mirati.

Capitolo 3

Protezione dei dati aziendali con l'AI: strategie e soluzioni pratiche

La protezione dei dati rappresenta una delle sfide più importanti per le imprese: le violazioni dei sistemi aziendali, infatti, possono causare danni economici significativi e compromettere la reputazione dell'azienda.

Il report di Capgemini "New defenses, new threats: What AI and Gen AI bring to Cybersecurity" frutto di un'indagine condotta su 1.000 organizzazioni basate in 13 Paesi, tra cui l'Italia, e attive in 12 settori, offre una **panoramica sulla percezione della Cybersecurity da parte delle aziende** e sul potenziale contributo dell'Intelligenza Artificiale in questo ambito. Oltre il 60% delle imprese intervistate ha registrato una riduzione di almeno il 5% nel tempo di rilevamento delle minacce dopo aver implementato soluzioni basate sull'AI nei propri centri operativi di sicurezza. Quasi il 40%, inoltre, ha riportato una diminuzione simile nel tempo di ripristino a seguito di incidenti di sicurezza.

Per fornire una panoramica esaustiva sullo stato dell'arte delle PMI sull'argomento, risulta utile affiancare a questi dati quelli divulgati da ISTAT. Nel **2024**, in **Italia**, è aumentata la quota di imprese con almeno 10 addetti che ha **adottato una più vasta gamma di strumenti di sicurezza informatica**: il 32,2% delle imprese (28,0% nel 2022) dichiara di utilizzare almeno sette delle 11 misure di sicurezza analizzate.
Le misure in questione riguardano:

- autenticazione con password complessa;
- backup separato dei dati;
- controllo dell'accesso alla rete;
- conservazione dei file di registro;
- VPN;
- monitoraggio delle attività sospette;
- almeno due sistemi di autenticazione;
- valutazione del rischio ICT;
- test di sicurezza ICT;
- crittografia dati, documenti o e-mail;
- metodi biometrici.

Nel 2023, **il 75,9% delle imprese italiane con almeno 10 dipendenti ha adottato almeno tre misure di sicurezza**, un dato in linea con la media europea (76,5%). Anche le aziende più piccole hanno dato importanza alla Cybersecurity, privilegiando strumenti meno sofisticati come l'autenticazione con password forte (86,6%) e il backup dei dati (79,5%). Le soluzioni avanzate, invece, sono rimaste meno diffuse, con solo il 44,7% delle imprese che conserva i file di registro per l'analisi degli incidenti, il 36,9% che effettua valutazioni del rischio e il 31,8% che realizza test periodici di sicurezza.

L'adozione di misure più evolute cresce, ma resta dunque limitata: la crittografia per dati, documenti o e-mail raggiunge il 23,9%, mentre i metodi biometrici di autenticazione si fermano al 12,1%.
Di fronte a uno scenario come quello odierno, dove le minacce cyber crescono è importante, anzi necessario, **investire in sicurezza**, anche per le piccole e medie imprese che hanno bisogno di proteggere i loro sistemi per non incorrere in ingenti perdite.

Un **esempio emblematico** che mostra quanto nessuna realtà sia davvero al riparo è rappresentato dall'attacco subito da **Luxottica**, leader mondiale nella produzione di occhiali. Nel 2020, l'azienda è stata colpita da un **ransomware** che ha compromesso l'accesso a sistemi interni e cifrato documenti aziendali cruciali, costringendo alla chiusura temporanea di alcuni stabilimenti italiani. L'attacco ha messo in evidenza la fragilità anche delle infrastrutture più avanzate e ha avuto impatti diretti sulla produzione e sull'operatività quotidiana.

Per le PMI, questo episodio suona come un campanello d'allarme: se un'azienda di tale portata può essere messa in crisi da un attacco informatico, nessuna impresa può ritenersi immune. In questo scenario, l'integrazione di soluzioni AI-driven nei sistemi di sicurezza - in particolare nel monitoraggio delle minacce e nel rilevamento delle anomalie - rappresenta un'opportunità concreta per prevenire danni simili, grazie a **strategie e soluzioni scalabili e accessibili** che possono essere adattate alle specifiche esigenze di aziende con risorse più limitate.

3.1 Crittografia avanzata AI-driven

A fronte dell'aumento delle minacce informatiche, **la crittografia** - ossia la tecnica che rende i dati incomprensibili a chi non ne ha l'autorizzazione - **si è trasformata in un pilastro essenziale per la protezione dei dati aziendali**. Tuttavia, i metodi tradizionali presentano limiti di adattabilità e possono risultare vulnerabili a nuove tecniche di attacco. Qui entra quindi in gioco l'Intelligenza Artificiale, che rivoluziona il settore con algoritmi crittografici più evoluti, capaci di offrire una sicurezza più robusta e reattiva.

Un aspetto determinante dell'Intelligenza Artificiale applicata alla crittografia è la sua **capacità di adattarsi dinamicamente alle minacce emergenti**. I sistemi AI-driven analizzano costantemente il traffico di rete e il comportamento degli utenti, regolando i protocolli crittografici in base al rischio rilevato. In caso di attività sospette, possono aumentare il livello di cifratura in tempo reale o modificare automaticamente le strategie di protezione per evitare vulnerabilità note. Questa **flessibilità** rappresenta un grande vantaggio rispetto ai sistemi tradizionali, che spesso richiedono aggiornamenti manuali e risultano meno reattivi agli attacchi più sofisticati.

Inoltre, l'AI permette di **individuare e correggere falle nei sistemi crittografici** prima che possano essere sfruttate dagli hacker. Grazie all'analisi predittiva e al monitoraggio continuo, le aziende sono così in grado di scoprire tentativi di attacco nel momento stesso in cui si verificano, bloccare accessi sospetti e automatizzare gli aggiornamenti di sicurezza per garantire sempre la massima protezione disponibile.

L'integrazione dell'Intelligenza Artificiale nei sistemi di crittografia rappresenta, quindi, un passo decisivo per rafforzare la sicurezza dei dati aziendali, rendendo le PMI meno vulnerabili alle minacce informatiche.

3.2 Analisi predittiva delle minacce

In questo contesto, ciò che rende **l'analisi predittiva** potenziata dall'AI davvero innovativa nel proteggere le imprese dai rischi informatici, è la sua capacità di andare oltre il semplice rilevamento: permette, infatti, di "guardare nel futuro", aiutando le imprese a reagire agli attacchi e, soprattutto, a prevenire che accadano. Come osservato nei capitoli precedenti, ad esempio, attraverso algoritmi di Machine Learning, l'AI può analizzare i dati provenienti da attacchi passati e identificare comportamenti ricorrenti o anomalie che potrebbero essere indicative di minacce imminenti. Questa capacità di previsione è basilare per contrastare attacchi come i ransomware o i malware che mirano a sfruttare falle conosciute nei sistemi.

Un esempio pratico di come l'analisi predittiva potrebbe intervenire per evitare rischi informatici, è l'ondata di attacchi ransomware registrata contro alcune PMI venete.

Nel **febbraio 2025**, oltre **30 piccole e medie imprese in Veneto**, attive nei settori manifatturiero, medicale e moda, sono state vittime di una **serie coordinata di attacchi ransomware**. I cybercriminali, appartenenti al gruppo Akira, hanno sfruttato vulnerabilità nei firewall e credenziali compromesse per infiltrarsi nelle reti aziendali, crittografare i dati e bloccare l'operatività.

L'impatto è stato grave: interruzione delle attività produttive, perdita temporanea di accesso a documenti riservati e richieste di riscatto che andavano da 100.000 a 400.000 euro per il ripristino dei dati. In alcuni casi, le aziende colpite hanno impiegato diversi giorni per tornare operative, con evidenti ricadute economiche e reputazionali.

Un elemento comune a molte delle imprese coinvolte è stata l'**assenza di sistemi di rilevamento comportamentale**, ovvero strumenti capaci di monitorare costantemente le attività degli utenti e identificare anomalie in tempo reale, come accessi fuori orario, trasferimenti massivi di dati o esecuzioni sospette.

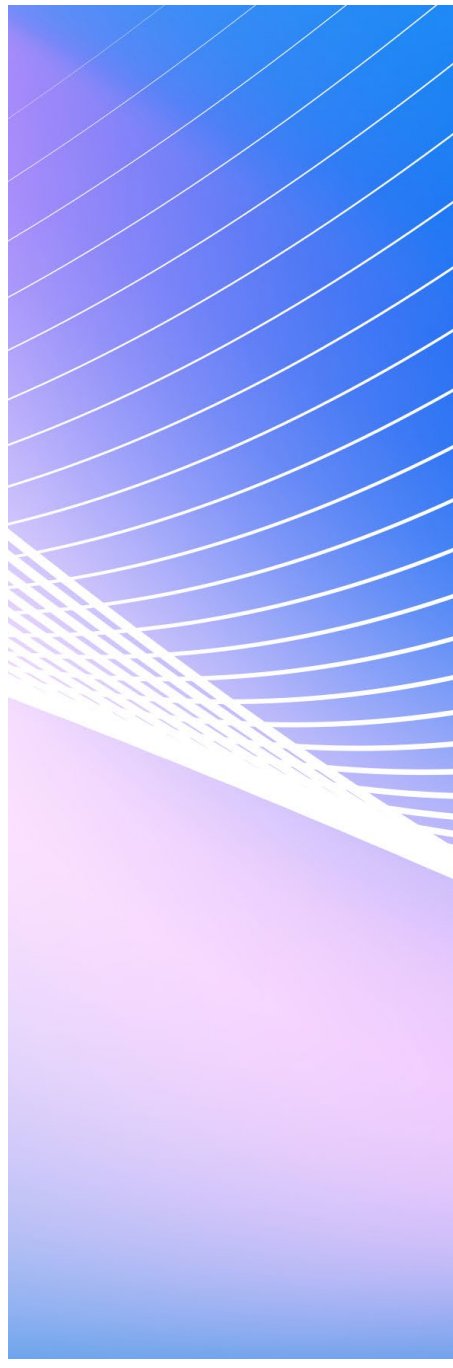
Questo episodio dimostra come l'adozione di soluzioni AI-driven in grado di riconoscere comportamenti anomali e attivare contromisure automatiche può rappresentare una svolta decisiva per intercettare le minacce prima che causino danni irreversibili.

Ma la potenza dell'analisi predittiva non si limita alla sola rilevazione: è anche in grado di **automatizzare la risposta alle minacce**. In un contesto dove il tempo di risposta è fondamentale per limitare i danni, l'Intelligenza Artificiale consente alle aziende di agire tempestivamente senza necessità di un intervento umano immediato. Questo approccio automatizzato riduce i tempi di reazione e accresce l'efficacia nel mitigare i rischi.

Inoltre, grazie all'apprendimento continuo, **l'AI migliora costantemente le sue previsioni, diventando sempre più precisa nell'identificare le minacce** prima che si trasformino in danni concreti. Con questa tecnologia, le aziende possono affrontare con maggiore serenità il futuro della sicurezza informatica, mettendo in atto difese più robuste e intelligenti.

3.3 Zero Trust Security

La **Zero Trust Security è un modello di difesa** che sfida l'idea di fiducia implicita all'interno delle reti aziendali. A differenza dei sistemi di sicurezza tradizionali, che spesso assumono che gli utenti all'interno della rete siano affidabili, questo modello **si basa sul principio che nessuno, nemmeno all'interno dell'azienda, debba essere considerato automaticamente fidato**. Ogni richiesta di accesso a un sistema, che provenga da un utente interno o esterno, deve essere rigorosamente verificata: l'obiettivo principale di questo approccio è quello di ridurre al minimo i rischi, prevenendo l'accesso non autorizzato e limitando i danni derivanti da possibili attacchi.



Un aspetto chiave della Zero Trust Security è, quindi, il **monitoraggio continuo degli accessi**: le imprese che implementano questa filosofia non solo controllano chi ha accesso ai loro sistemi, ma lo fanno costantemente, utilizzando tecnologie come l'analisi comportamentale e l'Intelligenza Artificiale. Ogni accesso viene verificato in base a una serie di parametri (come l'ora, la posizione e il dispositivo utilizzato) e, se qualcosa appare sospetto o fuori dall'ordinario, l'accesso può essere immediatamente negato, minimizzando il rischio di compromissioni. Il monitoraggio continuo aiuta quindi a rilevare attività anomale e a rispondere tempestivamente a possibili minacce, prima che possano evolvere in danni più gravi.

Un altro principio fondamentale della Zero Trust Security è l'adozione dell'**autenticazione biometrica** - ovvero un tipo di identificazione che si basa su caratteristiche fisiche uniche dell'utente, come l'impronta digitale, il riconoscimento facciale o la scansione dell'iride - per **garantire un controllo rigoroso sugli accessi**. A differenza delle password tradizionali, che possono essere facilmente rubate o indovinate, le credenziali biometriche sono estremamente difficili da falsificare. In un contesto Zero Trust, l'autenticazione biometrica aiuta a verificare l'identità dell'utente e svolge quindi un ruolo cruciale nella prevenzione degli attacchi. In questo modo, infatti, anche se un malintenzionato riuscisse ad acquisire le credenziali di un dipendente, non sarebbe comunque in grado di accedere ai sistemi aziendali.

Tutto ciò dimostra come l'adozione del modello Zero Trust possa migliorare la sicurezza di un'azienda, proteggendo dati sensibili e garantendo la continuità operativa anche in un contesto di minacce informatiche in continua evoluzione.

Approfondimento

Violazioni dei dati: impatti concreti per aziende e clienti

Nel 2023, come evidenziato dall'Identity Theft Resource Center, si sono registrate 3.205 violazioni dei dati, che hanno compromesso le informazioni personali e i dati di 353 milioni di persone, segnando un incremento significativo rispetto agli anni precedenti. Il caso più eclatante è stato quello di T-Mobile, con 37 milioni di vittime, seguito da Xfinity e PeopleConnect. Il settore sanitario, in particolare, è stato oggetto di numerosi attacchi, ma la minaccia ha interessato anche i settori finanziari e quello dei servizi professionali. Un dato da sottolineare è che oltre 2.365 di queste violazioni sono state causate da attacchi informatici, il che conferma la crescente sofisticazione dei criminali informatici.

L'impatto di una violazione dei dati aziendali non è mai sottovalutabile. Da un lato, le aziende coinvolte subiscono danni reputazionali e legali notevoli, che possono tradursi in perdite economiche immediate. Ad esempio, i costi legati alla notifica ai clienti, alla gestione delle crisi e alle eventuali sanzioni normative (come il GDPR) sono considerevoli. Nel caso delle aziende sanitarie, come CareSource e Premier Health, ad esempio, l'esposizione di dati sensibili come le informazioni mediche ha condotto a cause legali costose, danni permanenti alla fiducia dei clienti e rischi per la privacy degli utenti.

Dall'altro lato, per i clienti le conseguenze sono altrettanto considerevoli.
La violazione dei dati può comportare:

- furto d'identità;
- accesso non autorizzato ai conti bancari;
- utilizzo fraudolento delle informazioni personali;

I clienti, infatti, rischiano di subire danni economici diretti e perdite legate alla loro reputazione. Le violazioni dei dati, come quelle che hanno colpito milioni di utenti di T-Mobile, rendono più facile per i criminali informatici monetizzare i dati rubati, utilizzandoli per compiere attacchi di phishing, estorsione o vendite illegali di informazioni.

Capitolo 4

Come l'AI ridefinisce le strategie di sicurezza aziendale

Come abbiamo potuto analizzare nei capitoli precedenti, un approccio proattivo e strutturato alla sicurezza informatica è fondamentale per proteggere dati e asset aziendali.

Le ultime due edizioni del Cybersecurity Trends di Gartner hanno confermato la bontà di questa osservazione, evidenziando come **entro il 2026 le organizzazioni che adotteranno programmi di gestione continua delle minacce informatiche riusciranno a ridurre del 66% il rischio di subire violazioni**. Ma non solo. Gartner prevede, inoltre, che le aziende che sapranno **combinare l'utilizzo della Generative AI** - ovvero di tecnologie basate sull'Intelligenza Artificiale in grado di creare nuovi codici o modelli e, di conseguenza, di simulare scenari di rischio, generare analisi predittive o creare modelli comportamentali, tesi ad aumentare la consapevolezza degli utenti e migliorare le pratiche di sicurezza all'interno dell'organizzazione - con programmi di formazione in materia di sicurezza riusciranno a ridurre del 40% gli incidenti causati da comportamenti errati dei dipendenti.

L'integrazione dell'AI nella Cybersecurity, quindi, non riguarda semplicemente l'adozione di nuove tecnologie, ma **implica un cambiamento strategico** nel modo in cui le aziende affrontano la sicurezza digitale. In questo capitolo esploreremo tre temi centrali quando si parla di AI e sicurezza: come l'AI sta diventando un elemento imprescindibile nella strategia di sicurezza delle imprese, l'importanza della formazione continua per affrontare i nuovi scenari digitali e le principali sfide che l'uso dell'AI pone nel campo della Cybersecurity.

4.1 L'AI come elemento chiave nella strategia aziendale

Come abbiamo visto, l'Intelligenza Artificiale si è ormai trasformata in un vero e proprio "**collaboratore digitale**" per le aziende, capace di unire velocità di azione e precisione delle risposte. Grazie a queste caratteristiche, l'AI si afferma come uno strumento indispensabile nella protezione delle infrastrutture digitali, soprattutto in un contesto in cui le minacce informatiche sono sempre più complesse e rapide a evolversi.

Integrata nei sistemi di Cybersecurity, l'AI è in grado, inoltre, di **monitorare costantemente l'intero ecosistema aziendale**, intercettando attività sospette e vulnerabilità prima che possano tradursi in violazioni effettive. Tra le principali funzionalità operative offerte dall'AI troviamo:

individuazione precoce di anomalie e vulnerabilità, con un sistema di allerta anticipata che previene i danni;

analisi contestuale del rischio, attraverso l'interpretazione intelligente delle minacce, distinguendo i veri pericoli dai falsi allarmi;

implementazione o suggerimento automatico di contromisure, come il blocco di accessi sospetti, l'isolamento di dispositivi compromessi o l'aggiornamento immediato delle patch di sicurezza;

comunicazione chiara e sintetica delle minacce, traducendo analisi complesse in indicazioni semplici e azionabili, anche per chi non possiede competenze tecniche avanzate. Questa capacità di sintesi e personalizzazione rende la Cybersecurity più accessibile e permette alle organizzazioni di reagire in modo più rapido ed efficace, riducendo il rischio di danni reputazionali ed economici.

Tuttavia, per esprimere pienamente il suo potenziale, l'AI ha bisogno di un'**infrastruttura adeguata in grado di gestire ed elaborare grandi volumi di dati in tempo reale**. È qui che entra in gioco il **Cloud**: una componente fondamentale che fornisce alle aziende la potenza di calcolo necessaria per supportare i modelli di Intelligenza Artificiale. Grazie al Cloud, infatti, le imprese possono accedere a risorse scalabili e flessibili senza dover investire in costose infrastrutture hardware, rendendo le soluzioni AI più accessibili anche per realtà di piccole e medie dimensioni.

Inoltre, il Cloud consente **aggiornamenti continui dei sistemi di AI**, assicurando che le difese siano sempre allineate all'evoluzione delle minacce. Questo approccio dinamico permette alle aziende di rafforzare la propria resilienza digitale, migliorando la capacità di risposta agli attacchi, riducendo i tempi di inattività operativa e limitando al minimo le perdite economiche.

4.2. L'importanza della formazione

Come abbiamo visto, l'implementazione delle più moderne soluzioni di sicurezza informatica è essenziale, ma non sufficiente a proteggere un'azienda dalle minacce digitali. Un aspetto che non dovrebbe mai essere trascurato è quello della **formazione del personale**, in particolare nelle piccole e medie imprese, che spesso non dispongono di un reparto IT specializzato. È cruciale che le aziende investano nella formazione continua dei propri dipendenti, affinché possano comprendere, utilizzare e rispondere correttamente alle minacce informatiche.

A questo proposito, i dati forniti nel 2024 dall'Agenzia Europea per la Sicurezza Informatica ci permettono di avere il quadro aggiornato della situazione. Nonostante il 71% delle aziende riconosca la sicurezza informatica come una priorità assoluta, **il 74% non ha intrapreso alcuna azione di formazione**, lasciando i propri dipendenti sprovvisti della consapevolezza necessaria per fronteggiare le cyber minacce e affrontare le sfide informatiche attuali. Inoltre, il 68% delle aziende ha dichiarato che non è necessaria alcuna formazione o sensibilizzazione sulla Cybersecurity, mentre addirittura il 16% non è a conoscenza di opportunità di formazione pertinenti e **soltanto l'8% cita i vincoli di budget** come motivo di questo forte ritardo al riguardo.

Un collaboratore non adeguatamente formato può, senza rendersene conto, diventare il punto di accesso per minacce che mettono a rischio l'intera rete aziendale, i dati sensibili e, di conseguenza, anche la reputazione dell'organizzazione. Gli aggressori, infatti, puntano proprio sulla vulnerabilità umana: non sempre è necessario un sofisticato malware per violare un sistema; spesso **basta un'azione sbagliata di un dipendente ignaro**. Per questo motivo, la formazione in materia di Cybersecurity non deve essere considerata un evento isolato, ma un processo continuo e sistematico: ogni dipendente, indipendentemente dal ruolo o dal livello tecnico, deve essere coinvolto attivamente nello sviluppo di una cultura aziendale orientata alla sicurezza.

In questo contesto entra in gioco l'**upskilling** - ovvero il continuo aggiornamento delle competenze - che deve mirare non solo a insegnare regole e procedure, ma a far maturare nei collaboratori una vera consapevolezza del valore dei dati e della responsabilità individuale nella loro protezione.

Una formazione che può ritenersi efficace dovrebbe coprire diversi aspetti pratici, tra cui:

- **riconoscimento e prevenzione degli attacchi di phishing**, imparando a identificare e-mail sospette, siti web contraffatti e tentativi di ingegneria sociale (ovvero quelle tecniche di manipolazione psicologica utilizzate dai cyber criminali per ottenere informazioni confidenziali o accesso a sistemi protetti, che inducono le persone a compiere azioni che normalmente non farebbero, come rivelare password, fornire dati personali o scaricare software dannosi);

- **corretta gestione delle password**, adottando pratiche come l'uso di password robuste, l'attivazione dell'autenticazione a due fattori e l'utilizzo di password manager;

- **adozione di comportamenti sicuri nell'uso quotidiano degli strumenti digitali**, comprese le piattaforme cloud, le VPN e gli strumenti di collaborazione aziendale;

- **comprensione dei protocolli di segnalazione**, ovvero sapere come comportarsi e a chi rivolgersi in caso di incidente legato alla sicurezza informatica o sospetto di violazione.

Investire nella formazione significa, quindi, non solo ridurre il rischio di attacchi, ma anche costruire un'organizzazione più resiliente, dove ogni individuo si sente parte attiva nella difesa della sicurezza digitale aziendale. Ma non solo, la sensibilizzazione e la formazione delle risorse in materia di protezione passa anche attraverso l'adozione di soluzioni di cybersicurezza: più l'impresa investe in questo senso, più i dipendenti ne percepiscono l'importanza e ne sposano la causa.

4.3 Sfide dell'AI nella Cybersecurity

Accanto ai vantaggi garantiti dall'integrazione dell'Intelligenza Artificiale nei sistemi di Cybersecurity, esistono anche una serie di sfide lanciate dall'applicazione delle nuove tecnologie, che richiedono una **gestione attenta e una valutazione equilibrata dei rischi**. Se da un lato l'AI può offrire una protezione avanzata e reattiva contro minacce informatiche sempre più articolate, dall'altro non è esente da possibili criticità che, se non affrontate correttamente, possono compromettere la sicurezza stessa.

Uno dei principali rischi legati all'adozione dell'AI nella Cybersecurity è il potenziale **"overfitting"** (che si verifica quando un modello di Intelligenza Artificiale si adatta troppo ai dati su cui è stato allenato, al punto da imparare anche i dettagli che non sono importanti) o l'errore di **interpretare come minaccia comportamenti o pattern che non sono effettivamente dannosi**. Un'AI mal configurata o addestrata su dati insufficienti potrebbe generare falsi positivi, creando un errato allarme che porta a interventi inutili, rallentando - di conseguenza - i processi aziendali.

Un altro rischio non trascurabile dell'automazione è la **vulnerabilità agli attacchi mirati contro l'AI stessa**, in quanto i cybercriminali potrebbero sfruttare le debolezze nei modelli di Machine Learning per manipolare i dati e "ingannare" l'algoritmo, facendolo agire in modo dannoso o inatteso. Ciò rappresenta una minaccia esponenziale, poiché i sistemi di Intelligenza Artificiale che si basano su feedback automatico potrebbero auto-sabotarsi se subiscono attacchi ben studiati.

Per bilanciare l'AI con il controllo umano, le imprese devono quindi adottare un **approccio ibrido**. La tecnologia dovrebbe essere utilizzata per monitorare, analizzare e rispondere a eventi di sicurezza, ma le decisioni finali, in particolare quando si tratta di rispondere ad attacchi complessi o a situazioni ambigue, dovrebbero essere prese da **esperti umani**. Questo approccio garantisce che le capacità cognitive, il giudizio esperto e la comprensione del contesto possano integrare l'automazione, riducendo il rischio di errori.

Per saperne di più:

→ Formazione continua: ottimizzare i percorsi formativi dei dipendenti con l'AI
→ Come implementare l'Intelligenza Artificiale in azienda: i requisiti
→ Gestire e garantire la sicurezza informatica anche con lo smart working

Approfondimento

OEC, la multinazionale che ha puntato sulla formazione per ridurre il rischio di cyberattacchi

OEC, gruppo internazionale attivo nell'ingegneria e costruzioni con sedi in Brasile e in diversi Paesi, si è trovata di fronte a una sfida crescente: l'**aumento degli attacchi di phishing** diretti ai propri dipendenti e ai partner di progetto. L'azienda gestisce cantieri complessi, appalti milionari e una supply chain globale: un singolo clic errato avrebbe potuto mettere a rischio dati sensibili, continuità operativa e reputazione. Inoltre, il personale è distribuito su più nazioni e parla lingue diverse, il che rendeva difficile mantenere uno standard uniforme di consapevolezza sulla sicurezza informatica.

Per rispondere a questa esigenza, OEC ha avviato un **programma strutturato di formazione e sensibilizzazione sulla Cybersecurity**. Il progetto ha previsto un roll-out internazionale di corsi multilingua, con contenuti formativi brevi, pratici e contestualizzati al lavoro quotidiano. Parallelamente sono state introdotte **campagne periodiche di phishing simulato** – differenziate per Paese e funzione aziendale – per misurare il livello di rischio reale e individuare le aree più vulnerabili. È stato anche integrato un pulsante di segnalazione ("*Phish Alert*") nelle caselle di posta aziendali, per facilitare la comunicazione tempestiva con l'IT.

I risultati si sono visti in tempi rapidi. A soli tre mesi dal baseline iniziale, l'azienda ha registrato una **riduzione di oltre l'80% nel tasso di clic ai test di phishing**, segno di un cambiamento concreto nei comportamenti. Il 94% dei dipendenti coinvolti ha completato i moduli di formazione previsti e sono state erogate complessivamente più di 1.600 ore di training. La maggiore capacità di riconoscere e segnalare le email sospette ha migliorato anche i tempi di risposta interna, contribuendo a **ridurre il rischio complessivo di compromissione**.

Conclusioni

La sicurezza informatica non si configura più soltanto come un adempimento tecnico, ma come **una leva strategica per crescere e innovare senza paura**.

Come abbiamo visto in questo documento, soluzioni che integrano al proprio interno modelli di **Intelligenza Artificiale offrono alle PMI l'opportunità di proteggere il proprio futuro** con strumenti potenti ma accessibili, trasformando la sicurezza da mera necessità a vantaggio competitivo.

Per garantire, quindi, una crescita sostenibile alla propria impresa è fondamentale che la Cybersecurity sia integrata nelle strategie aziendali. Ciò implica l'**allineamento degli obiettivi di sicurezza con quelli di business**, l'impegno attivo della leadership e l'adozione di un approccio proattivo nella gestione dei rischi. Solo in questo modo, le imprese possono proteggere i propri asset e costruire, di pari passo, una reputazione solida e affidabile sul mercato.

Per facilitare questo processo le PMI dovranno pertanto:

- **mappare le vulnerabilità**, identificando i punti deboli nei sistemi aziendali attraverso audit regolari;
- **selezionare soluzioni tecnologiche adeguate**, valutando strumenti basati sull'Intelligenza Artificiale che si adattino alle specifiche esigenze dell'azienda, considerando fattori come scalabilità e facilità d'uso;
- **investire nella formazione continua**, promuovendo una cultura della Cybersecurity attraverso sessioni formative periodiche per sensibilizzare il personale sulle minacce emergenti e sulle best practice di sicurezza.

Tuttavia, il futuro della sicurezza informatica non si giocherà solo sul piano tecnologico, ma anche su quello etico e culturale. L'adozione dell'AI impone nuove responsabilità: occorre **garantire trasparenza nei processi decisionali automatizzati, protezione della privacy**, e prevenzione di abusi derivanti da un uso improprio dell'Intelligenza Artificiale stessa. La regolamentazione diventerà un elemento chiave per equilibrare innovazione e tutela dei diritti.

Un ulteriore elemento imprescindibile sarà la **centralità dell'essere umano**. Per quanto avanzate siano le tecnologie, la sicurezza rimane un processo profondamente umano, basato su consapevolezza, responsabilità e capacità critica. Nessun algoritmo potrà sostituire completamente la sensibilità, l'intuito e il senso etico di una persona formata e attenta.

Insomma, investire nelle giuste competenze e tecnologie non significa solo difendersi dalle minacce, ma anche **abbracciare con fiducia le infinite possibilità del digitale**. La vera forza di un'azienda, piccola o grande che sia, non risiede solo nei suoi prodotti o servizi, ma nella capacità di evolversi e adattarsi a scenari in continua trasformazione. E in questo processo, la sicurezza informatica — intelligente, adattiva e umana — sarà il motore invisibile che alimenterà la fiducia, l'innovazione e la resilienza aziendale.

Glossario

Access point
Dispositivo che consente a computer, smartphone o altri terminali di connettersi a una rete informatica, spesso wireless. È un punto di ingresso che, se non protetto adeguatamente, può diventare vulnerabile ad attacchi esterni.

AI-driven
Tecnologie o processi in cui l'AI non solo supporta, ma guida attivamente le operazioni, prendendo decisioni o suggerendo azioni sulla base dei dati analizzati in tempo reale.

Alert
Segnalazione automatica generata da un sistema informatico in risposta a un'attività sospetta o pericolosa. Gli alert sono fondamentali per il monitoraggio della sicurezza e l'attivazione di contromisure tempestive.

Analisi predittiva
Metodo analitico che utilizza dati storici e modelli statistici o di machine learning per anticipare eventi futuri, come tentativi di intrusione o anomalie nei sistemi informatici.

Antivirus
Software progettato per individuare, bloccare e rimuovere programmi dannosi, come virus, worm o trojan. I più evoluti integrano funzionalità basate su AI per riconoscere minacce non ancora catalogate.

Authentication (Autenticazione)
Processo che verifica l'identità di un utente o di un dispositivo prima di consentire l'accesso a un sistema. Può essere basata su password, biometria, token fisici o comportamenti digitali.

Autenticazione biometrica
Metodo che utilizza caratteristiche fisiche uniche dell'utente (ad es. impronta digitale, volto, voce) per confermare l'identità in modo più sicuro rispetto alle credenziali tradizionali.

Backup
Copia di riserva di dati o sistemi, conservata per consentire il ripristino in caso di perdita, attacco ransomware o malfunzionamento. I backup vanno eseguiti regolarmente e tenuti separati dalla rete principale.

Behavioral analysis (Analisi comportamentale)
Tecnica che monitora i comportamenti abituali di utenti o dispositivi e segnala deviazioni potenzialmente indicative di un attacco, come accessi in orari insoliti o trasferimenti anomali di dati.

Cloud
Infrastruttura tecnologica remota e virtualizzata accessibile tramite Internet. Piuttosto che utilizzare server o software installati localmente, i dati e i servizi risiedono in data center esterni – gestiti da fornitori specializzati – a cui è possibile accedere in tempo reale da qualsiasi luogo e dispositivo autorizzato. Il Cloud consente alle aziende di archiviare file, eseguire applicazioni e processi, creare ambienti virtuali e collaborare in modo flessibile, con un abbattimento dei costi legati all'acquisto e alla manutenzione di hardware fisico.

Crittografia
Tecnologia che codifica i dati rendendoli illeggibili a chi non possiede la chiave di decodifica. Serve a proteggere informazioni sensibili durante la trasmissione o l'archiviazione.

Crittografia avanzata AI-driven
Sistemi di cifratura che, grazie all'AI, si adattano dinamicamente al rischio, modificando i protocolli o intensificando la protezione in presenza di minacce o anomalie.

Cybersecurity
Insieme di tecnologie, processi e pratiche utilizzate per proteggere reti, dispositivi, sistemi e dati da attacchi informatici, accessi non autorizzati o danni intenzionali.

Dark web
Parte non indicizzata di Internet accessibile solo tramite software specifici (es. Tor), spesso usata per attività illecite come la vendita di dati rubati o strumenti di hacking.

Glossario

Data breach (Violazione dei dati)
Accesso, uso o divulgazione non autorizzata di dati sensibili. Può avere gravi conseguenze legali, economiche e reputazionali per le aziende coinvolte.

Data center
Struttura fisica che ospita server, dispositivi di rete e sistemi di storage, garantendo la continuità operativa e la sicurezza fisica e logica delle infrastrutture IT aziendali.

Deepfake
Contenuto multimediale (audio, video, immagini) generato o manipolato tramite AI per imitare persone reali in modo credibile, spesso con finalità fraudolente.

Firewall
Sistema che filtra il traffico in entrata e in uscita da una rete aziendale, bloccando le connessioni non autorizzate o potenzialmente pericolose.

Generative AI
Ramo dell'AI capace di creare contenuti originali (testi, immagini, video, codice), a partire da input testuali o dati grezzi. Viene usata anche per generare simulazioni o scenari di attacco.

Hybrid environments
Ambienti IT misti in cui coesistono infrastrutture on-premises (in sede) e servizi cloud, spesso interconnessi per ottimizzare costi e prestazioni.

Incident response
Insieme di attività pianificate per rilevare, analizzare, contenere e risolvere un incidente di sicurezza informatica, limitando i danni e ripristinando la normalità.

Intelligenza Artificiale (AI)
Tecnologia che consente ai sistemi informatici di simulare capacità cognitive tipiche dell'uomo, come apprendere, ragionare, pianificare o prendere decisioni. Nella cybersecurity, è utilizzata per analizzare grandi volumi di dati, individuare anomalie e prevenire minacce.

Machine Learning
Tecnica dell'AI che consente ai sistemi di migliorare le proprie prestazioni analizzando dati, senza essere esplicitamente programmati. È la base dell'automazione nella cybersecurity predittiva.

Malware
Categoria di software malevolo che include virus, trojan, spyware, ransomware. Viene usato per rubare dati, danneggiare sistemi o prendere il controllo di dispositivi.

On-premises
Infrastruttura IT installata fisicamente all'interno dell'azienda, sotto il suo controllo diretto (si contrappone al modello Cloud).

Patch
Aggiornamento software rilasciato per correggere vulnerabilità, errori o migliorare la sicurezza di un'applicazione o sistema operativo.

Phishing
Tecnica fraudolenta che utilizza e-mail, messaggi o siti falsi per indurre l'utente a rivelare informazioni sensibili come credenziali d'accesso o dati bancari.

Ransomware
Tipo di malware che cripta i dati aziendali e chiede un riscatto (ransom) per decrittarli. Una delle minacce più diffuse e dannose per le PMI.

Risk management (Gestione del rischio)
Processo continuo che identifica, valuta e mitiga i rischi potenziali per gli asset aziendali, compresi quelli informatici.

Security breach
Violazione delle difese di sicurezza informatica, con possibile compromissione dei sistemi, accessi non autorizzati o sottrazione di dati.

Glossario

Security Operations Center (SOC)
Unità aziendale o esterna dedicata al monitoraggio costante degli eventi di sicurezza, all'analisi delle minacce e alla gestione degli incidenti informatici.

Social Engineering
Tecniche di manipolazione psicologica volte a ingannare le persone per ottenere accesso a sistemi, dati o risorse protette. Il phishing ne è un esempio tipico.

Supply chain attack
Attacco che sfrutta vulnerabilità nei fornitori o partner per colpire indirettamente l'azienda target. È in forte crescita a causa dell'interconnessione tra imprese.

Threat Hunting
Attività proattiva condotta dagli esperti di sicurezza per individuare minacce nascoste nei sistemi prima che si manifestino in modo evidente.

Threat Intelligence
Processo di raccolta, analisi e condivisione di informazioni sulle minacce informatiche per prevenirle e rispondere con maggiore efficacia.

VPN (Virtual Private Network)
Tecnologia che crea un canale cifrato tra l'utente e la rete aziendale, proteggendo i dati durante la navigazione su reti pubbliche o non sicure.

Zero Trust Security
Modello di sicurezza che si basa sul principio che nessuno – nemmeno chi è dentro la rete – debba essere considerato affidabile per impostazione predefinita. Ogni accesso deve essere verificato.

Zero-day
Vulnerabilità di sicurezza sconosciuta al produttore del software e già sfruttata dagli hacker. Sono tra le minacce più pericolose perché non ancora risolte.

Fonti

- **Istat.it**
  https://www.istat.it/wp-content/uploads/2025/01/Statreport_ICT2024-1.pdf
- **Clusit.it**
  https://clusit.it/rapporto-clusit/
- **Mixmode.ai**
  https://mixmode.ai/state-of-ai-in-Cybersecurity-2024/
- **Security.ntt**
  https://www.security.ntt/blog/2024-annual-cyber-security-report
- **Cfodive.com**
  https://www.cfodive.com/news/smbs-risk-shutting-down-cyberattack-ai-Cybersecurity/743405/
- **Aipsi.org**
  https://www.aipsi.org/aree-tematiche/osservatorio-attacchi-digitali/oad-2024/rapporto-oad-2024-pubblicato-e-scaricabile.html
- **Capgemini.it**
  https://www.capgemini.com/news/press-releases/ai-and-gen-ai-are-set-to-transform-Cybersecurity-for-most-organizations/
- **Osservatori.net**
  https://www.osservatori.net/insight/digital-identity/riconoscimento-elettronico-grandi-aziende-italiane-insight/
- **Governing.com**
  https://www.governing.com/management-and-administration/2023-will-go-down-for-record-setting-number-of-data-breaches
- **Gartner.com**
  https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartner-identifiesthe-top-Cybersecurity-trends-for-2025
- **Digital-strategy.ec.europa.eu**
  https://digital-strategy.ec.europa.eu/en/news/eu-must-reinforce-Cybersecurity-skills
- **Kasperskydaily.com**
  https://media.kasperskydaily.com/wp-content/uploads/sites/86/2024/05/23140825/Enterprise_Cybersecurity_Report_23-05-24-1.pdf
- **Marketsandmarkets.com**
  https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-ai-cyber-security-market-220634996.html

Fonti

- **Cybsersecurity360.it**
  https://www.Cybersecurity360.it/nuove-minacce/Cybersecurity-2025-rapporto-clusit-dati-tendenze/

  https://www.Cybersecurity360.it/soluzioni-aziendali/attacchi-sofisticati-difendersi-con-intelligenza-artificiale-machine-learning-e-automazione/

  www.Cybersecurity360.it/soluzioni-aziendali/Cybersecurity-come-mettere-in-sicurezza-le-aziende/

  https://www.Cybersecurity360.it/nuove-minacce/in-cassa-integrazione-per-colpa-del-ransomware-sempre-piu-casi-in-italia

  https://www.Cybersecurity360.it/soluzioni-aziendali/sicurezza-adattiva-cose-e-perche-e-utile-per-prevedere-e-prevenire-i-cyber-attacchi/

- **Ponemonsullivanreport.com**
  https://ponemonsullivanreport.com/2024/04/the-2024-study-on-the-state-of-ai-in-Cybersecurity/

- **Wired.it**
  https://www.wired.it/article/leonardo-machine-learning-Cybersecurity-economia/

- **Bloomberg.com**
  https://www.bloomberg.com/news/articles/2024-07-26/ferrari-narrowly-dodges-deepfake-scam-simulating-deal-hungry-ceo?

- **Key4biz.it**
  https://www.key4biz.it/pmi-un-dipendente-su-due-non-sa-riconoscere-una-email-di-phishing-e-con-lo-smart-working-la-minaccia-aumenta/525016/

- **Corrierecomunicazioni.it**
  https://www.corrierecomunicazioni.it/cyber-security/intelligenza-artificiale-per-la-Cybersecurity-il-giro-daffari-annuale-crescera-del-219/

Potenzia la
tua **Impresa**.

Eleva il tuo business[AI]

con i software TeamSystem,
ora potenziati
dall'Intelligenza Artificiale.

TeamSystem

teamsystem.com

OFFICINE BONFIGLIOLI

TeamSystem

VERS.01 - DIC.2025

teamsystem.com