N. 132

DIRECTION

LE TECNOLOGIE CHE MUOVONO IL BUSINESS

TUTTI PAZZI per l'AI

EASYNET GROUP
LA CULTURA DATA-DRIVEN RACCONTATA DA ALBERTO VASSENA

SENTINELONE
PER LA SICUREZZA IT OCCORRE UN APPROCCIO GLOBALE

SOPHOS DORA: LA SFIDA DELLA CYBERSECURITY

OPENTEXT
LA SICUREZZA REINVENTATA: L'AI COME ALLEATA PER LA PROTEZIONE AZIENDALE

MERCATI VERTICALI - FINANCE La rivoluzione digitale della finanza e dei servizi bancari
DORA: opportunità e sfide per il settore finanziario **a cura di IDC**

snom

A330D

SP800

D865

M500

M56

Benvenuto nell'universo della flessibilità!

I telefoni IP Snom offrono una qualità audio eccellente, un'esperienza utente intuitiva e massima sicurezza delle conversazioni, anche in ambienti "remote desktop".

www.snom.com

INDICE

DIRECTION
Anno XXI - numero 132
Febbraio 2025
Direttore responsabile: Riccardo Florio
Coordinamento editoriale: Paola Rosa
Ha collaborato: Maurizio Ferrari, Fabrizio Pincelli, Stefano Uberti Foppa
Redazione: Via Gorizia 35/37 20099 Sesto San Giovanni (MI); Tel 339 3785157; https://reportec.it; redazione@reportec.it

Immagini: Dreamstime.com
Stampa: New Press Edizioni Srl - Via Della Traversa, 22 - 22074 Lomazzo (CO)
Editore: Reportec Srl; C.so Italia 50 20122 Milano
Il Sole 24 Ore non ha partecipato alla realizzazione di questo periodico e non ha responsabilità per il suo contenuto
Amministratore unico: Riccardo Florio
Iscrizione al tribunale di Milano n° 212 del 31 marzo 2003
Diffusione cartacea + digitale 32.500 copie

Reportec è una società fondata da Gaetano Di Blasio, Riccardo Florio, Giuseppe Saccardi

L'**AI** E IL FUTURO QUOTIDIANO TRA **RIVOLUZIONE** E **ILLUSIONE**

di Riccardo Florio
• *direttore responsabile* •

Parliamo ancora di intelligenza artificiale perché non è proprio possibile farne a meno. L'acronimo AI o AI (all'inglese) è ormai sulla bocca di tutti. Ogni giorno leggiamo articoli, seguiamo dibattiti e ascoltiamo esperti parlare di AI come la grande rivoluzione del nostro tempo. I produttori di tecnologia sono impegnati più che mai su questo tema, anche se al netto di annunci e "hype", l'adozione da parte delle aziende di applicazioni capaci di essere realmente disruptive per il business non è ancora molto diffusa.

A un'altra velocità procede, invece, l'uso personale dell'AI. Mentre molte aziende faticano a trasformare questa tecnologia in un vantaggio competitivo concreto, il consumatore medio si sta già abituando a interagire con l'AI in modo sempre più naturale: assistenti virtuali, strumenti di generazione di testi e immagini, chatbot conversazionali e così via.

L'AI promette, infatti, di cambiare in modo profondo sia il mondo del lavoro sia la vita delle persone. Per esempio, automatizza mansioni ripetitive, aiuta nella presa di decisioni, ottimizza processi e offre un supporto senza precedenti in settori come la sanità, la sicurezza e la produzione industriale. Mentre in alcuni ambiti il cambiamento è tangibile, in altri si naviga ancora tra speranze e promesse. **Ci si interroga su etica, rischi, regolamentazione, ma intanto il mondo corre. I colossi che dominano il commercio mondiale** stanno già implementando l'AI a livello industriale. Amazon, per esempio, utilizza algoritmi avanzati per ottimizzare la logistica e la gestione delle scorte, riducendo sprechi e costi operativi. Tesla sfrutta il machine learning per migliorare le capacità di guida autonoma dei suoi veicoli, con aggiornamenti software continui che affinano le performance delle auto già in circolazione. Nel settore sanitario, l'AI viene già impiegata per diagnosticare patologie con un livello di precisione superiore a quello umano: strumenti come Google DeepMind hanno dimostrato di poter individuare malattie oculari con un'accuratezza del 94%.

L'AI NEL NOSTRO FUTURO QUOTIDIANO

Il futuro che ci aspetta dietro l'angolo potrebbe essere non solo molto diverso dall'attuale ma anche molto vicino. Avventuriamoci nell'immaginario e **proviamo a prevedere una giornata tipo, tra qualche anno, in un mondo pervaso dall'AI**.

Ti svegli e la tua AI personale ha già analizzato il tuo sonno, suggerendoti quando alzarti e cosa mangiare per ottimizzare le tue energie. Il

tuo assistente digitale ti aggiorna sulle notizie selezionate in base ai tuoi interessi, mentre il tuo sistema domotico regola illuminazione e temperatura in base alle tue abitudini.
Durante il lavoro, **le riunioni sono ottimizzate: non devi più scrivere report, perché un algoritmo trascrive e sintetizza i punti chiave.**
Le mail di routine vengono filtrate, redatte e inviate in automatico. Perfino le decisioni strategiche aziendali vengono prese con il supporto di modelli predittivi avanzati.
I mezzi di trasporto autonomi ci porteranno ovunque desideriamo, eliminando lo stress della guida. Durante il viaggio l'AI ci accompagnerà indirizzandoci verso i nostri svaghi digitali preferiti o suggerendoci nuovo acquisti in linea con le nostre abitudini. Le città saranno attraversate da veicoli senza conducente, coordinati da un'intelligenza artificiale che ottimizzerà i percorsi per ridurre il traffico e l'inquinamento.
La musica non sarà più semplicemente ascoltata, ma creata su misura per ogni utente: basterà esprimere un'emozione o uno stato d'animo e l'AI comporrà in tempo reale una colonna sonora personalizzata.
Lo stesso accadrà con i film: non più esperienze passive, ma vere e proprie avventure interattive vissute in prima persona grazie a visori immersivi. Gli attori? Saranno entità digitali, modellate dall'AI per incarnare qualsiasi ruolo, senza limiti di età, genere o nazionalità.
Arrivando a casa, troveremo la spesa già depositata nel nostro box dedicato, ordinata in autonomia dall'AI, che avrà monitorato le nostre abitudini alimentari per garantirci una scorta ottimale dei nostri cibi preferiti, evitando sprechi e dimenticanze. La programmazione delle vacanze? Uno scherzo da ragazzi con l'AI.
Perfino le relazioni personali potrebbero essere stravolte. Non è azzardo pensare che molte persone sceglieranno la sicurezza di interagire con compagni virtuali invece di affrontare l'onere di una relazione tradizionale: avatar guidati dall'AI per comprendere, sostenere e interagire in modo empatico, offrendo un'alternativa sempre più allettante alle dinamiche relazionali reali.
Anche nel mondo dell'arte e della creatività, l'AI si farà strada. **Le opere d'arte generate da algoritmi diventeranno indistinguibili da quelle create dall'uomo**, con autori virtuali capaci di dipingere, scrivere poesie e comporre sinfonie.
Il concetto di originalità sarà ridefinito e le opere d'arte saranno frutto di calcoli statistici più che di ispirazione umana.

MA SARÀ DAVVERO COSÌ?

Ma sarà davvero così? Riuscirà il potere di persuasione della tecnologia a scardinare la nostra voglia di autenticità, di relazioni vere e di esperienze non mediate da un algoritmo?
Ci saranno ambiti in cui **l'intelligenza artificiale non riuscirà a entrare, come la spiritualità e la religione**, che restano dimensioni profondamente umane, legate a percezioni e significati che sfuggono alla logica dell'algoritmo.
L'AI potrà simulare la fede, ma non viverla.
Potrà anche azzardarsi a dare risposte alle domande esistenziali, ma non colmare il bisogno di senso che solo la coscienza umana può soddisfare o perlomeno inseguire. Alla fine, il vero interrogativo non è se l'AI prenderà il sopravvento, ma se noi **saremo ancora in grado di scegliere la vita reale rispetto all'illusione di una perfetta simulazione.**

ARCHIVIAZIONE SICURA DEI DATI **ON-PREMISE** E NEL **CLOUD**

LA GESTIONE SICURA DEI DATI È UNA PRIORITÀ PER LE AZIENDE MODERNE, DIVISE TRA SOLUZIONI ON-PREMISE E CLOUD. UN APPROCCIO IBRIDO PERMETTE DI COMBINARE CONTROLLO DIRETTO E SCALABILITÀ, MENTRE L'ADOZIONE DI TECNOLOGIE AVANZATE, COME CRITTOGRAFIA E AI, RAFFORZA LA PROTEZIONE DELLE INFORMAZIONI.

DI MERCEDES OLEDIEU

Il rapido mutamento del panorama ICT, spinto dalla continua evoluzione tecnologica e dall'incremento delle minacce informatiche, impone alle imprese di rivedere le proprie strategie di archiviazione dati per garantire protezione, continuità operativa e flessibilità. La scelta tra infrastrutture on-premise, soluzioni cloud e modelli ibridi non riguarda solamente l'adozione di tecnologie all'avanguardia, ma **implica anche una valutazione approfondita degli aspetti economici, organizzativi e di compliance**. In questo scenario, il business manager, deve individuare la soluzione più idonea alle esigenze specifiche della propria realtà dovendo bilanciare investimenti in hardware, spese operative e la necessità di garantire una protezione costante contro rischi e vulnerabilità, in linea con le normative vigenti.

IL MODELLO ON-PREMISE: CONTROLLO TOTALE E INVESTIMENTI DIRETTI

Le soluzioni on-premise continuano a rappresentare una scelta strategica per quei settori che richiedono un controllo completo sulle infrastrutture e sui dati sensibili, dove le aziende dispongono della completa proprietà delle infrastrutture hardware e dei relativi processi di sicurezza. Dotarsi di data center interni consente di personalizzare le configurazioni e le politiche di sicurezza, offrendo **una gestione "in house" che, in alcuni ambiti risulta indispensabile per rispettare normative rigorose** (come quello finanziario, sanitario e della Pubblica Amministrazione). Tuttavia, la gestione di sistemi on-premise comporta investimenti iniziali elevati e una spesa operativa costante, dovuta anche all'aggiornamento periodico di hardware e software.
Le implicazioni in termini di costi operativi e di capitale rappresentano un fattore critico, soprattutto per le PMI che non dispongono delle risorse necessarie per sostenere infrastrutture complesse.

IL CLOUD: FLESSIBILITÀ, SCALABILITÀ E SICUREZZA DINAMICA

Dall'altra parte, le soluzioni cloud offrono un'alternativa dinamica e scalabile, in grado di garantire elevati standard di sicurezza attraverso l'adozione di sistemi aggiornati in tempo reale e la gestione condivisa della sicurezza tra provider e azienda.
I principali provider, infatti, investono in tecnologie di crittografia avanzata, autenticazione multifattoriale e monitoraggio in tempo reale, **garantendo che le risorse siano sempre protette contro le minacce emergenti.**
Il Flexera 2023 State of the Cloud Report ha evidenziato come il 76% delle organizzazioni intervistate abbia registrato benefici rilevanti nella gestione dei costi operativi grazie alla migrazione verso il cloud, inclusi quelli collegati alla sicurezza dei dati.
Inoltre, il modello di spesa pay-per-use tipico del cloud consente alle imprese di adeguare gli investimenti alle effettive necessità operative, eliminando oneri iniziali massicci e rendendo la gestione finanziaria più flessibile.

L'ARCHIVIAZIONE IBRIDA: IL MEGLIO DI ENTRAMBI I MONDI

Per molte organizzazioni, l'adozione di un modello ibrido rappresenta la soluzione ottimale, in quanto consente di sfruttare le peculiarità di entrambi gli approcci. Integrando infrastrutture on-premise con servizi cloud, le aziende possono **ottenere il meglio di entrambi i mondi**: da un lato, il controllo diretto sui dati più critici e la personalizzazione tipici delle infrastrutture locali, dall'altro la scalabilità, la flessibilità e la capacità di risposta rapida agli incidenti offerte dai servizi cloud.
In contesti in cui la localizzazione geografica dei dati assume un'importanza cruciale per la conformità normativa, la scelta di soluzioni cloud private o ibride permette di scegliere dove e come conservare le informazioni sensibili, pur beneficiando della potenza e della resilienza operativa del cloud pubblico.
La continua evoluzione del settore ICT porta con sé l'adozione di tecnologie emergenti che stanno rivoluzionando il modo di archiviare e proteggere i dati. **L'impiego di intelligenza artificiale e machine learning**, per esempio, consente di analizzare in tempo reale enormi volumi di dati, rilevando

comportamenti anomali e intervenendo prontamente per contenere potenziali minacce. Soluzioni di backup e disaster recovery basate su algoritmi predittivi migliorano la capacità di risposta delle infrastrutture, riducendo significativamente i tempi di ripristino dopo un attacco o un guasto tecnico.

L'APPROCCIO INTEGRATO GARANTISCE RESILIENZA E COMPETITIVITÀ

La costante trasformazione nel panorama delle architetture per l'archiviazione dei dati richiede **una visione strategica che consideri non solo l'aspetto tecnologico, ma anche le implicazioni economiche e normative**. La crescente complessità degli ambienti digitali e la diffusione di attacchi informatici mirati hanno spinto il settore a innovare, sviluppando soluzioni sempre più sofisticate e integrate.

Le organizzazioni che sapranno bilanciare con attenzione il controllo offerto dall'on-premise e la flessibilità del cloud, sfruttando al meglio le potenzialità dei modelli ibridi, saranno in grado di garantire continuità operativa e protezione dei dati, elementi imprescindibili per navigare con successo in un mercato altamente competitivo.

In un'epoca in cui la sicurezza informatica è al centro delle preoccupazioni manageriali, **scegliere il giusto mix di soluzioni tecnologiche diventa quindi una priorità** per chi intende non solo proteggere i propri asset, ma anche valorizzare le opportunità di innovazione e crescita offerte dalla trasformazione digitale. In tale contesto, **un approccio integrato,** capace di coniugare la solidità del controllo interno con la dinamicità delle tecnologie cloud, rappresenta una scelta strategica destinata che si configura non soltanto come una risposta alle esigenze attuali, ma come un investimento a lungo termine **in grado di garantire resilienza e competitività in un ecosistema digitale in costante trasformazione.**

LE 10 BEST PRACTICE PER L'ARCHIVIAZIONE SICURA

Indipendentemente dall'approccio scelto, la sicurezza dell'archiviazione dei dati deve basarsi su un framework solido. Ecco le 10 pratiche da cui non è possibile prescindere.

1. **Crittografia e tokenizzazione dei dati:** proteggere i dati a riposo e in transito con crittografia avanzata per evitare accessi non autorizzati e adottare tecniche avanzate di mascheramento per limitare l'accesso ai dati reali senza comprometterne l'usabilità.
2. **Controllo degli accessi ai dati Zero Trust:** presupporre che nessun utente o dispositivo sia implicitamente affidabile e implementare il principio del minimo privilegio e l'autenticazione a più fattori per proteggere l'accesso ai dati sensibili.
3. **Backup regolari e sicuri:** effettuare copie di backup frequenti, conservandole in più luoghi e proteggendole con crittografia per prevenire perdita di dati.
4. **Implementazione di politiche di retention:** definire e applicare politiche di conservazione e cancellazione dei dati per rispettare i requisiti normativi e ridurre i rischi.
5. **Monitoraggio dell'integrità dei dati:** utilizzare strumenti di controllo per verificare che i dati archiviati non subiscano alterazioni non autorizzate.
6. **Protezione contro ransomware e malware:** adottare soluzioni di rilevamento e prevenzione per evitare attacchi che possano compromettere i dati archiviati.
7. **Segmentazione dell'archiviazione:** organizzare i dati in compartimenti separati per ridurre il rischio di compromissione generalizzata in caso di attacco.
8. **Gestione sicura del ciclo di vita dei dati:** garantire che i dati vengano archiviati, utilizzati e smaltiti secondo le migliori pratiche di sicurezza.
9. **Conformità alle normative di protezione dei dati:** assicurarsi che le soluzioni di archiviazione rispettino regolamenti come GDPR, ISO 27001 e altre normative settoriali.
10. **Test e simulazioni di recovery:** eseguire periodicamente prove di ripristino dei dati per assicurarsi che i backup siano efficaci e accessibili in caso di emergenza.

Il 17 gennaio 2025, il Digital Operational Resilience Act è diventato pienamente operativo, segnando un passo cruciale nella gestione dei rischi informatici per il settore finanziario europeo.

DORA: LA SFIDA DELLA CYBERSECURITY

a cura di Marco D'Elia di Sophos

Le entità finanziarie sono tra le più esposte agli attacchi informatici, non da ultimo per la posta in gioco associata alla loro attività e per la loro natura essenziale. Secondo i dati del FMI, il settore finanziario ha subito più di 20.000 attacchi informatici, con perdite per quasi 12 miliardi di dollari. In risposta, le autorità europee hanno approvato un nuovo regolamento, il Digital Operational Resilience Act (DORA), che stabilisce un approccio coordinato e omogeneo alla sicurezza informatica per le entità finanziarie dell'Unione Europea. Entrato in vigore lo scorso 17 gennaio, DORA comporta complesse sfide di conformità per le entità finanziarie, che devono adattare rapidamente le loro infrastrutture e i loro processi per soddisfarne i requisiti, ma rappresenta anche un'opportunità per rafforzare la sicurezza informatica, in particolare circondandosi di partner esperti e affidabili che consentano loro di rafforzare la propria resilienza informatica e di prepararsi ad affrontare le sfide presenti e future della sicurezza informatica.

VERSO UNA SICUREZZA INFORMATICA IN AMBITO FINANZIARIO SEMPRE PIÙ COERENTE E RESILIENTE

La maggior parte delle entità finanziarie, dispone di sistemi IT legacy che rendono difficile l'integrazione di complessi standard di cybersecurity. Inoltre, la normativa richiede l'implementazione di controlli continui sulla sicurezza informatica che probabilmente prosciugheranno le risorse finanziarie e umane degli operatori finanziari. Queste difficoltà dimostrano chiaramente la necessità per le istituzioni finanziarie di affidarsi a soluzioni tecniche avanzate e a risorse esterne. Grazie alle competenze degli esperti di cybersecurity, le aziende possono ottimizzare la loro conformità, ridurre i rischi e rispondere in modo più efficace ai requisiti DORA. Gli istituti finanziari devono mettere in atto una forma di cybersecurity proattiva, utilizzando soluzioni di rilevamento e risposta agli incidenti rapide ed efficaci e rafforzare la gestione degli incidenti, riducendo altresì al minimo i rischi associati ai fornitori terzi. Rivolgendosi a esperti di sicurezza informatica, le entità finanziarie possono mettere in atto sistemi di gestione delle crisi più efficaci, assicurandosi al contempo di monitorare costantemente le soluzioni e la salute digitale dei propri fornitori. Collaborando con partner esperti, che si qualificano correttamente come CTPP, le entità finanziarie possono fare del DORA una leva strategica per rafforzare la loro cybersecurity e aumentare la propria resilienza in un panorama di minacce informatiche in continua evoluzione.

Per informazioni

MARCO D'ELIA
COUNTRY MANAGER
SOPHOS ITALIA

PER LA **CYBERSECURITY** NON BASTA UN PRODOTTO, SERVE UNA **PIATTAFORMA**

Lo afferma Marco Rottigni, technical director di SentinelOne, che illustra come per erigere un'efficace protezione contro gli attacchi dei cybercriminali serve ricorrere a una soluzione che deve prevedere almeno quattro elementi essenziali

DI FABRIZIO PINCELLI

Oggi, gli attacchi dei cybercriminali hanno raggiunto una tale sofisticatezza che per assicurare un elevato livello di protezione bisogna ricorrere a piattaforme complete e integrate, che prevedono l'uso di diversi sistemi, ciascuno ottimizzato per identificare e bloccare un determinato tipo di minaccia o abilitare una specifica protezione. Nasce quindi la necessità di poter gestire le informazioni che arrivano da un parco eterogeneo, riuscendo a discriminare i reali attacchi da legittimi comportamenti degli utenti. Non solo. Tutto questo va fatto in tempi rapidissimi per non lasciare la possibilità agli attaccanti di andare a segno. Serve una velocità di detection che un uomo non può raggiungere, devono occuparsene i sistemi automatizzati. Ma come ottenere tali risultati? Abbiamo posto questa e altre domande a **Marco Rottigni, technical director di SentinelOne**.

D COSA VUOL DIRE ATTUARE LA CYBERSECURITY OGGI?

Oggi per massimizzare l'efficacia con cui si erige la difesa dagli attacchi avanzati del cybercrime non si deve più parlare di singola soluzione ma di piattaforma. Sono ancora tante le persone che identificano SentinelOne con l'Endpoint detection & response (EDR): è stata e rimane una delle nostre eccellenze. Tuttavia, oltre all'EDR, una piattaforma di difesa oggi deve avere almeno altri tre componenti altrettanto validi: un **SIEM** (Security information and event management) potenziato dall'intelligenza artificiale che deve capire da dove è arrivato l'attaccante e se l'attacco è ancora in corso o è stato debellato; un **data lake** di back-end che riceve le telemetrie da tutti gli agent presenti in rete (anche di vendor differenti, quindi che usano linguaggi diversi) e un sistema di **AI generativa** che sappia analizzare rapidamente tali dati, effettuando anche interrogazioni complesse, così da avere più velocemente possibile un'indicazione di quanto sta succedendo. La nostra piattaforma di cybersecurity si chiama **Singularity** e la nostra proposta in tema di intelligenza artificiale generativa è **Purple AI**.

D QUALI VANTAGGI COMPORTA L'IMPIEGO DELL'AI GENERATIVA?

L'introduzione dell'AI generativa nella nostra piattaforma consente di tradurre richieste effettuate anche di tipo complesso usando il linguaggio naturale in query avanzate, migliorando significativamente le capacità analitiche e accelerando le indagini dell'analista. La normalizzazione dei dati, resa possibile anche dall'adozione dello standard OCSF (Open cybersecurity schema framework), garantisce una maggiore coerenza e facilita l'analisi trasversale tra diverse fonti, come potrebbero essere i log creati da

sistemi di diversi e molteplici vendor, quali per esempio Palo Alto, Check Point, Fortinet o CyberArk, per citare alcuni dei più noti. L'AI generativa non si limita però alla creazione di query: è in grado di contestualizzare eventi specifici all'interno di una sequenza più ampia, fornendo agli analisti una comprensione approfondita e riducendo i loro tempi di reazione.

D UNA DELLE VOSTRE NOVITÀ PIÙ ATTESE PER IL 2025 È L'HYPER AUTOMATION. IN COSA CONSISTE?

L'hyper automation arriverà a breve ed è un altro pilastro fondamentale della nostra piattaforma.
In pratica è un'automazione avanzata che permette di orchestrare flussi di lavoro complessi tramite un **approccio no-code**, rendendo accessibile la configurazione anche a utenti con competenze tecniche limitate. Con oltre 150 configurazioni preimpostate per l'integrazione trasparente di tecnologie di terze parti senza costi aggiuntivi, la piattaforma supporta una vasta gamma di sistemi, inclusi Office 365, Google Suite e firewall aziendali, garantendo una rapida implementazione e una risposta coordinata alle minacce.
È un approccio che supera i limiti tradizionali dei SOAR (Security orchestration automation and response), eliminando la necessità di lunghi processi per la personalizzazione di flussi di lavoro codificati e riducendo i costi associati. In questo gioca un ruolo essenziale l'approccio no-code che permette letteralmente di avere a disposizione un insieme di mattoncini da assemblare per automatizzare determinati flussi di lavoro.

MARCO ROTTIGNI,
TECHNICAL DIRECTOR
DI SENTINELONE

D LA SEMPLICITÀ, NELL'IMPLEMENTAZIONE E NELL'UTILIZZO, ASSUME UN RUOLO CHIAVE...

Esatto. SentinelOne Singularity consente agli analisti di interrogare i dati in modo unificato e di ottenere una visione globale delle attività sospette, rendendo più efficaci le operazioni di rilevamento e risposta. La nostra piattaforma è compatibile con un'ampia varietà di sistemi operativi, inclusi Windows, Mac e Linux, e supporta anche versioni obsolete come Windows 7 e Windows Server 2003. L'installazione non richiede il riavvio della macchina, minimizzando l'impatto sulle operazioni aziendali e garantendo una transizione fluida. In questo, gioca un ruolo fondamentale anche la collaborazione con partner qualificati, che è un elemento centrale della nostra strategia. Attraverso i Managed security service provider (MSSP), possiamo offrire soluzioni chiavi in mano, permettendo alle organizzazioni di ogni dimensione di adottare la tecnologia in modo flessibile. Ciò consente anche a piccole realtà, come gli studi professionali, di accedere a una protezione avanzata senza dover gestire direttamente l'infrastruttura di sicurezza.

LA SICUREZZA REINVENTATA: L'**AI COME ALLEATA** PER LA PROTEZIONE AZIENDALE

La cybersecurity si trasforma adottando un approccio proattivo che sfrutta l'intelligenza artificiale per proteggere le aziende, ridurre i rischi e contrastare le minacce in tempo reale

DI RICCARDO FLORIO

Con la crescente complessità dello scenario digitale, la sicurezza informatica è diventata una sfida strategica per le aziende di ogni settore. Le minacce si evolvono rapidamente, sfruttando vulnerabilità sempre più difficili da individuare. Per affrontare questa realtà servono **strategie di protezione avanzate, capaci di integrare analisi predittiva e intelligenza artificiale per prevenire attacchi** prima ancora che si verifichino.

OpenText Cybersecurity si posiziona all'avanguardia, offrendo soluzioni integrate che spaziano dalla protezione contro il ransomware alla sicurezza del codice alimentata dall'intelligenza artificiale. Attraverso l'integrazione di intelligenza artificiale e analisi avanzate diventa possibile rilevare comportamenti anomali, individuare lacune e adattare i controlli di sicurezza in tempo reale. Questo approccio proattivo permette di anticipare le minacce, anziché reagire a incidenti già avvenuti.

Inoltre, la gestione sicura delle informazioni è **cruciale per scoprire, classificare, governare, proteggere e archiviare dati sensibili**, garantendo il rispetto delle normative e la conformità ai regolamenti di settore.

"Le aziende non possono più considerare la sicurezza informatica un semplice strato di protezione, - osserva **Pierpaolo Alì, Southern director OpenText Cybersecurity** - *ma devono vederla come un ecosistema dinamico, in grado di adattarsi in tempo reale alle minacce emergenti. L'intelligenza artificiale, integrata in un'architettura di cybersecurity avanzata, non solo rafforza le difese, ma permette di individuare pattern di attacco che sfuggirebbero ai tradizionali sistemi di sicurezza."*

PROTEZIONE DEL CODICE E SICUREZZA APPLICATIVA: L'AI COME ACCELERATORE DELLA DIFESA

La sicurezza del codice rappresenta una delle sfide più critiche per le aziende digitali, poiché una vulnerabilità nel software può essere sfruttata per accedere a dati sensibili, compromettere sistemi o diffondere malware su vasta scala.

L'integrazione di **soluzioni avanzate di sicurezza applicativa basate sull'intelligenza artificiale** consente di identificare e risolvere vulnerabilità con una rapidità e una precisione mai raggiunte prima. Grazie alla capacità dell'AI di analizzare enormi quantità di codice e individuare anomalie difficili da rilevare con i metodi tradizionali, le aziende possono affrontare le minacce prima che possano essere sfruttate dagli attaccanti. A ciò si aggiunge l'esigenza di analizzare le componenti open source, ormai immancabili all'interno di ogni sviluppo software moderno.

La famiglia di soluzioni **Fortify** sviluppata da OpenText Cybersecurity risponde a queste sfide integrandosi nelle "toolchain" di sviluppo moderne e **sfruttando tecnologie di machine learning non supervisionato per automatizzare l'analisi del codice, fornire suggerimenti per la correzione delle vulnerabilità in tempo reale e controllare le vulnerabilità note delle librerie open source**.
Questo modello di sicurezza applicativa è pensato per una protezione intrinseca che si mantenga attraverso l'intero ciclo di vita del software: un requisito in linea con le indicazioni del modello DevSecOps.

Per la protezione dei dati sensibili OpenText Cybersecurity ha sviluppato **tecnologie avanzate di classificazione, mascheramento e cifratura** in grado di identificare automaticamente tramite l'AI dati critici e applicare le misure di protezione adeguate, riducendo l'esposizione a potenziali violazioni e rendendo inutilizzabili i dati anche in caso di sottrazione.
Attraverso questo modello reinventato di sicurezza, guidato dall'AI, integrato e proattivo le imprese possono non solo proteggersi dalle minacce attuali, ma anche prepararsi efficacemente per quelle future.

IDENTITÀ E DATI: PROTEZIONE E RISPOSTA RAPIDA NELL'ERA DELL'AI

L'adozione dell'AI introduce nuove sfide per la gestione delle identità e la protezione dei dati, rendendo essenziale un approccio avanzato per garantire sicurezza e conformità. Le soluzioni di OpenText comprendono strumenti sofisticati per il controllo degli accessi, implementando **meccanismi di autenticazione basati sull'intelligenza artificiale e sistemi di monitoraggio continuo per rilevare comportamenti sospetti,** colmare eventuali lacune e adattare in tempo reale i controlli di sicurezza. Grazie alla governance in tempo reale, le organizzazioni possono garantire che solo gli utenti autorizzati accedano alle risorse critiche, riducendo drasticamente il rischio di accessi non autorizzati.
Identificare e dare priorità alle minacce è cruciale per proteggere identità, dati e applicazioni, attraverso una gestione automatizzata della postura di sicurezza: un compito che deve essere eseguito con grande rapidità se si vogliono prevenire danni significativi. Anche in questo caso l'AI viene in aiuto consentendo di analizzare grandi volumi di dati in tempo reale e permettendo alle organizzazioni di rispondere prontamente agli incidenti.

PIERPAOLO ALÌ,
SOUTHERN DIRECTOR
OPENTEXT CYBERSECURITY

L'AI CAMBIA FACCIA ALLA CYBERSECURITY

Dalla generazione di malware polimorfici ai Deepfake fino alla protezione delle infrastrutture critiche, il panorama delle nuove minacce richiede strategie innovative e framework di sicurezza efficaci

DI RICCARDO FLORIO

PAOLO PALUMBO,
VP & HEAD DI WITHSECURE INTELLIGENCE

L'intelligenza artificiale non può essere considerata una novità nel settore della cybersecurity. Da anni, infatti, le aziende utilizzano il machine learning per affrontare la crescente mole di minacce informatiche, che sarebbe impossibile gestire manualmente. Tuttavia, fino al rilascio di ChatGPT nel novembre 2022, l'AI era uno strumento prevalentemente riservato agli addetti ai lavori. Con l'introduzione di un'interfaccia di utilizzo intuitiva basata sul linguaggio naturale, l'AI generativa è diventata accessibile a chiunque, innescando un'ondata di sperimentazione che ha generato sia applicazioni rivoluzionarie che rischi inediti.

Paolo Palumbo guida il team WithSecure Intelligence, un gruppo di esperti il cui compito è tracciare e analizzare le attività dei cybercriminali per trasformare queste informazioni in soluzioni di sicurezza avanzate. Il suo team include data scientist e specialisti in machine learning, impegnati a monitorare l'evoluzione del panorama delle minacce informatiche e a sviluppare strumenti di difesa sempre più efficaci.

I TRE VOLTI DELL'AI NELLA SICUREZZA INFORMATICA

"Nell'ambito dell'Information Security, noi di WithSecure Intelligence consideriamo l'AI da tre prospettive - osserva Palumbo -. *La prima è come* ***strumento di offesa*** *a disposizione di singoli utenti e aziende per automatizzare migliorare l'efficienza operativa delle attività criminali. La seconde è come* ***mezzo di difesa****, sfruttato per individuare e contrastare le minacce informatiche, contribuendo così alla protezione di aziende e istituzioni. Infine come possibile* ***elemento di rischio per sé stessa****, poiché l'AI può essere manipolata dai criminali per*

aggirare i sistemi di sicurezza, compiere operazioni di spionaggio o diffondere disinformazione".
Capire come i criminali informatici utilizzano l'AI non è semplice. Aziende come OpenAI e Google, con il loro accesso diretto ai modelli generativi, hanno una prospettiva privilegiata su queste dinamiche e i rapporti pubblicati da questi giganti della tecnologia mostrano come, attualmente, un suo uso per abilitare attacchi avanzati sia ancora raro, mentre **gli hacker stanno sfruttando l'AI soprattutto per ottimizzare attività come la creazione di malware, il phishing avanzato e il social engineering**. Alcuni gruppi, supportati da stati come Russia, Iran, Corea del Nord e Cina, hanno già iniziato a integrare questi strumenti nelle loro strategie.

I NUOVI RISCHI PORTATI DALL'AI

Uno degli utilizzi più diffusi dell'AI in ambito malevolo è il profiling avanzato delle persone, che consente di condurre attacchi mirati con estrema precisione. Deepfake sofisticati vengono già impiegati per frodi e disinformazione, come ha dimostrato il recente caso del **video di Kamala Harris con l'audio manipolato digitalmente ri-postato da Elon Musk** a milioni dei suoi follower. La facilità con cui si possono generare contenuti falsificati solleva interrogativi sulla sicurezza dell'informazione e sull'affidabilità delle fonti online.
Capire la portata del fenomeno è ulteriormente complicato dalla difficoltà di valutare la portata dell'**uso malevolo che si potrebbe fare dell'AI in modo indiretto**. Un esempio è l'uso dell'AIGen per individuare vulnerabilità nel software grazie alla sua capacità di analizzare grandi quantità di codice; si tratta di informazioni che possono essere utilizzate sia dagli sviluppatori per aumentare la sicurezza sia dai cybercriminali per ragioni opposte.
Un approccio, ancora sperimentale, che mostra le possibili evoluzioni delle minacce informatiche nel prossimo futuro è dato dai malware polimorfici capaci di modificare il programma. Un esempio è LLMorpher, un nuovo prototipo di malware che non contiene codice malevolo diretto, ma **in grado di sfruttare la connessione con un LLM per generare codice dannoso "on the fly"**, eludendo così i sistemi di rilevamento tradizionali.
Un altro aspetto spesso trascurato riguarda la **gestione dei dati inseriti nei modelli di AI**.
"Nessuno sa con precisione dove finiscono le informazioni che inserisco in ChatGPT e simili - fa osservare Paolo Palumbo -, *né chi vi può accedere o sotto quali condizioni. I report di OpenAI e Google confermano come, sotto certe condizioni, sia possibile analizzare i dati inseriti dagli utenti e ciò solleva legittime domande sulla privacy e sul rischio di esposizione di informazioni sensibili"*.

STRATEGIE DI MITIGAZIONE E FRAMEWORK DI SICUREZZA

Con l'AI che evolve rapidamente, l'adozione di strategie proattive, la collaborazione tra esperti di cybersecurity e l'implementazione di framework di mitigazione saranno elementi essenziali per affrontare le sfide del futuro. Sono in via di sviluppo **framework e tassonomie per classificare i rischi legati all'AI** e gestirli in modo efficace. L'MIT, per esempio, ha proposto un sistema per esplorare le minacce, suddividendole in categorie come attacchi malevoli, discriminazione, disinformazione e sicurezza dei sistemi.
A supporto di queste esigenze **WithSecure ha sviluppato Luminen**, una funzionalità di intelligenza artificiale generativa basata su un Large Language Model (LLM), integrata nativamente all'interno della piattaforma WithSecure Elements Cloud, che fornisce ai team IT e di cybersecurity spiegazioni in linguaggio naturale degli eventi di sicurezza, suggerendo le opportune azioni correttive e i miglioramenti necessari per rafforzare la postura di sicurezza.
"WithSecure è stata pioniera nell'utilizzo del machine learning e dell'intelligenza artificiale nella cybersecurity fin dal 2006 - ricorda **Carmen Palumbo, country sales manager di WithSecure Italia** -. *I nostri algoritmi e il trattamento dei dati rispettano i più alti standard europei in termini di qualità, conformità e severi protocolli di privacy."*

AI GENERATIVA E ANALISI PREDITTIVA

PERCHÉ NON SE NE PUÒ PIÙ FARE A MENO

DI FABRIZIO PINCELLI

OGGI LE AZIENDE DI OGNI SETTORE, PUBBLICO PRIVATO CHE SIA, POSSONO TRARRE GRANDI BENEFICI DAL RICORSO ALL'INTELLIGENZA ARTIFICIALE: È INFATTI IL MODO PIÙ EFFICACE PER MIGLIORARE L'EFFICIENZA OPERATIVA RIDUCENDO I COSTI. VEDIAMO PERCHÉ E QUALI AMBITI OPERATIVI POSSONO ESSERE MAGGIORMENTE AVVANTAGGIATI

Negli ultimi anni l'intelligenza artificiale (AI) ha compiuto progressi significativi. Al punto che si tende ancora a parlare genericamente di intelligenza artificiale, mentre in realtà questa tecnica elaborativa si è diversificata affinando le sue competenze per ambiti specifici. Così, oggi possiamo dire che esistono alcuni tipi di AI: i più utilizzati sono sicuramente l'**AI generativa** e l'**AI predittiva**, spesso chiamata analisi predittiva (predictive analytics). Queste, pur sfruttando il medesimo principio, che è quello dell'apprendimento automatico (machine learning), permettono di raggiungere obiettivi distinti.

COS'È L'AI GENERATIVA?

L'AI generativa rappresenta una delle evoluzioni più rivoluzionarie dell'intelligenza artificiale. Pur essendo un concetto relativamente recente (è assurta agli onori della cronaca solo da poco più di un anno), sta già dimostrando un potenziale senza precedenti.
L'AI generativa si distingue per la capacità di creare contenuti nuovi e originali, imitando lo stile e la profondità delle produzioni umane. Il processo di funzionamento si articola in due fasi principali: l'**addestramento** e la **generazione**. Durante l'addestramento, l'AI analizza un ampio set di dati, identificando strutture e modelli sottostanti (i cosiddetti Large language model - LLM). Successivamente, nella fase di generazione, utilizza queste conoscenze per creare contenuti nuovi che rispecchiano le caratteristiche apprese. Questo processo è reso possibile da tecniche avanzate come le **reti neurali profonde**, che simulano il funzionamento del cervello umano, consentendo all'AI di elaborare dati complessi e produrre risultati innovativi.

COS'È L'AI PREDITTIVA?

Un altro pilastro tecnologico che sta plasmando l'ambito aziendale (e non solo) è l'AI predittiva. Questa disciplina sfrutta **dati storici e algoritmi avanzati** per anticipare eventi futuri e supportare il processo decisionale aziendale.
Per garantire che si ottenga il massimo valore dall'intelligenza artificiale predittiva è necessario **impostare obiettivi chiari e definire precisi KPI**. Inoltre, si deve avere la garanzia di disporre di dati di qualità. Infatti, mentre l'AI generativa si concentra sulla creazione di contenuti originali, l'AI predittiva **analizza i dati esistenti per formulare previsioni**.
L'intelligenza artificiale predittiva può fornire un aiuto nel prevedere se un certo evento si verificherà o quale impatto quantitativo potrebbero avere più eventi. Queste soluzioni si basano principalmente su dati strutturati di eventi passati.

L'intelligenza artificiale generativa, invece, è progettata per generare contenuti nuovi sulla base degli input dell'utente e dei dati non strutturati su cui è stata addestrata. Anche questi modelli possono fornire risposte, ma più che altro come opinioni di carattere qualitativo.
La **sinergia tra AI generativa e analisi predittiva** offre vantaggi notevoli. In un impiego aziendale, l'AI generativa può integrare l'AI predittiva per ricavare valore dai dati strutturati e non strutturati. In questo caso, i modelli predittivi sono utilizzati per migliorare i processi e i risultati, mentre i modelli generativi sono impiegati per soddisfare i requisiti di contenuto di tali processi. Per esempio, i modelli generativi possono arricchire l'analisi predittiva simulando scenari complessi e fornendo dati sintetici per ottimizzare le previsioni.
Vediamo in termini pratici come il ricorso all'AI generativa e all'AI predittiva sta apportando benefici ad alcuni importanti ambiti, quali la Pubblica amministrazione, l'automotive, il manufacturing, la sanità, il retail e la logistica.

PA: VERSO UNA NUOVA ERA DI AUTOMAZIONE

L'adozione dell'AI generativa sta inaugurando una nuova fase di automazione all'interno della Pubblica amministrazione con l'obiettivo di migliorare i modelli operativi e la qualità dei servizi offerti ai cittadini.
Un esempio è l'impiego di **chatbot avanzati e assistenti virtuali**, che automatizzano le risposte alle richieste degli utenti. Grazie a questi strumenti, le amministrazioni sono in grado di fornire informazioni e supporto in tempo reale, riducendo significativamente i tempi di attesa e migliorando l'efficienza complessiva. Questa modalità operativa non si limita all'interazione con i cittadini ma si estende alla **gestione documentale**.
Attraverso tecnologie come il Natural language processing (NLP) e l'apprendimento automatico, è possibile analizzare e comprendere la struttura dei documenti amministrativi, automatizzare la redazione di bozze di delibere, verificare e validare documenti e persino estrarre conoscenza da enormi quantità di dati testuali.
L'AI predittiva, inoltre, offre un supporto prezioso per migliorare la **pianificazione e l'erogazione** dei servizi pubblici. Analizzando grandi volumi di dati, è possibile prevedere la domanda di servizi specifici, ottimizzando la gestione delle risorse e rispondendo tempestivamente alle necessità dei cittadini. Per esempio, queste tecniche possono essere utilizzate per rilevare frodi, migliorare le prestazioni e comprendere meglio il comportamento della popolazione, promuovendo una maggiore trasparenza e responsabilità.
In un futuro prossimo, si prevede l'adozione di assistenti virtuali sempre più avanzati, in grado di apprendere dalle interazioni precedenti e fornire risposte personalizzate con un alto livello di precisione.
Parallelamente, l'uso dell'analisi predittiva consentirà di anticipare tendenze demografiche e socioeconomiche, migliorando la pianificazione degli interventi e ottimizzando la distribuzione delle risorse.

AUTOMOTIVE: IL FUTURO DELLA GUIDA AUTONOMA

All'interno dell'**industria automobilistica** l'integrazione di tecnologie avanzate come l'AI generativa e l'AI predittiva non solo sta rivoluzionando la progettazione e la produzione ma anche l'interazione tra veicoli e conducenti, delineando un futuro in cui la personalizzazione e l'automazione saranno al centro dell'esperienza.
Più in dettaglio, l'**AI generativa** sta ottimizzando i **processi di design**, permettendo la creazione di modelli innovativi che migliorano **prestazioni, sicurezza ed efficienza**. Inoltre, facilita simulazioni avanzate e ottimizzazioni strutturali, riducendo i tempi di sviluppo. Questo, analizzando dati da sensori e immagini, può rilevare difetti minimi nei componenti, garantendo elevati standard produttivi. L'intelligenza artificiale aiuta anche a progettare i layout delle fabbriche per **massimizzare efficienza**, suggerendo il modo migliore per organizzare le attrezzature e il flusso di lavoro.
L'**AI predittiva**, invece, sta rivoluzionando il processo di manutenzione, monitorando lo stato dei veicoli tramite sensori IoT per **anticipare guasti e programmare interventi**. Questa capacità di previsione si estende anche ai veicoli autonomi, dove l'analisi in tempo reale di condizioni stradali e traffico consente decisioni informate, migliorando sicurezza ed efficienza.
Un esempio di come l'AI generativa stia trasformando l'**interazione tra conducente e veicolo** è rappresentato dagli assistenti virtuali. Alimentati dall'intelligenza artificiale, tramite comandi vocali permettono, per esempio, di regolare la temperatura, riprodurre musica od ottenere indicazioni stradali. Questo tipo di innovazione non solo migliora l'esperienza utente, ma apre nuove opportunità per la mobilità. Le auto a guida autonoma usano l'AI per percorrere le strade senza l'intervento umano. Si affidano a sensori, telecamere e computer per prendere decisioni. Questo, quando l'infrastruttura lo consentirà, gli permetterà anche di dialogare tra di loro per ottimizzare il traffico ed evitare collisioni.

MANUFACTURING: AUTOMAZIONE SMART E PRODUZIONE OTTIMIZZATA

Il **settore manifatturiero** è tra i più influenzati dall'introduzione dell'AI generativa e dall'AI predittiva: stanno rivoluzionando l'intero ciclo produttivo, dalla progettazione alla distribuzione.
L'**AI generativa** sta ridefinendo la progettazione dei prodotti attraverso la creazione di **design ottimizzati** per criteri specifici come peso, resistenza e materiali. L'uso di **gemelli digitali** consente alle aziende di simulare configurazioni di componenti, accelerando i tempi di sviluppo e migliorando le prestazioni complessive.
Parallelamente, l'**AI predittiva** migliora la manutenzione degli impianti produttivi, monitorando in tempo reale i macchinari per **prevedere guasti e ottimizzare l'efficienza** operativa. Questo approccio riduce i tempi di inattività, con significativi risparmi sui costi.
Un altro ambito di applicazione è la gestione della **supply chain**. L'analisi di dati storici e in tempo reale consente di prevedere fluttuazioni nella domanda, ottimizzando i livelli di inventario e la pianificazione della produzione. Inoltre, l'AI generativa aiuta a identificare difetti di produzione attraverso l'analisi di immagini e dati dei sensori.
Infine, l'AI generativa favorisce la formazione del personale e il supporto operativo, creando scenari simulati per l'addestramento e assistenti virtuali per fornire soluzioni in tempo reale durante le operazioni. In questo senso, un ruolo sempre più importante lo rivestirà la **realtà virtuale**, che permetterà di operare con gemelli digitali di oggetti fisici su vasta scala simulandone il comportamento reale.

SANITÀ: DIAGNOSI AVANZATE E GESTIONE PREDITTIVA DELLE MALATTIE

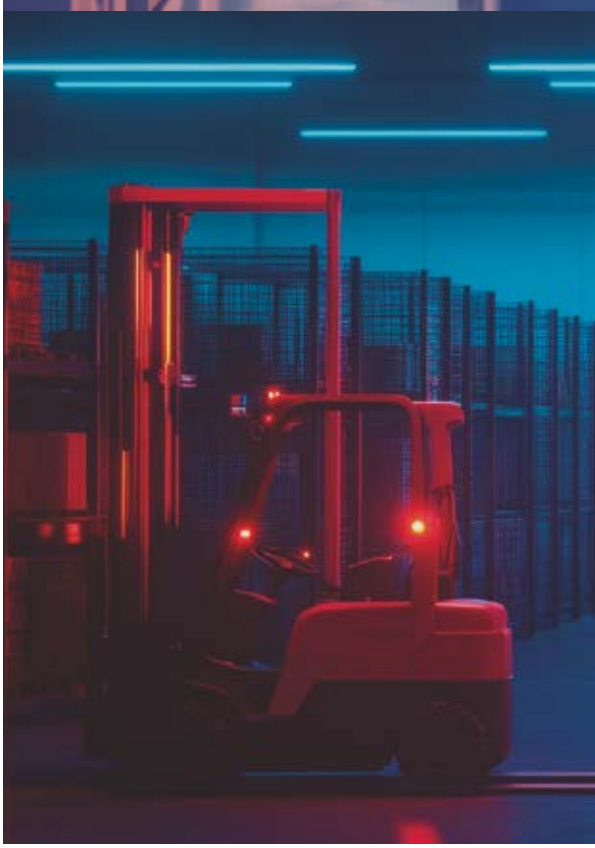
Nel **settore sanitario**, l'intelligenza artificiale generativa e predittiva consentono di creare strumenti innovativi per migliorare diagnosi, trattamenti e gestione delle risorse. Più in dettaglio, l'**AI generativa** risulta utile nella **progettazione di nuovi farmaci**, permettendo di simulare l'efficacia di composti chimici e accelerare il processo di scoperta. Inoltre, è impiegata per creare **terapie personalizzate**, adattando i trattamenti alle esigenze genetiche dei pazienti e migliorando l'efficacia dei risultati. Un altro ambito di impiego è l'automazione della documentazione medica. L'**AI predittiva** trova applicazione nella **diagnosi precoce** di condizioni patologiche, come il cancro, tramite l'analisi di dati genetici, ambientali e comportamentali. La capacità predittiva consente interventi tempestivi e migliora le probabilità di successo dei trattamenti. In più, monitorando pazienti con malattie croniche, è possibile prevedere complicazioni e ottimizzare la gestione delle risorse ospedaliere. Ciò porta benefici anche nelle terapie a distanza. Prova ne è che la nuova Piattaforma Nazionale di Telemedicina prevede l'uso dell'intelligenza artificiale. Risulta infatti strategico avere sotto controllo i parametri dei pazienti così da poter intervenire non appena le analisi predittive di tali parametri anticipano la possibilità che insorgano problemi.

RETAIL: SHOPPING PREDITTIVO E PERSONALIZZATO

Oltre ai modelli operativi, nel **settore retail**, l'AI generativa e l'AI predittiva stanno ridefinendo un aspetto essenziale: l'esperienza del cliente.
In tal senso, grazie all'**AI generativa** è possibile automatizzare la creazione di **contenuti personalizzati**, come descrizioni di prodotti e campagne di marketing, rendendo le informazioni più accessibili e coinvolgenti. Inoltre, con il ricorso a **chatbot intelligenti** si può offrire un'assistenza avanzata, guidando gli utenti e fornendo raccomandazioni su misura.
L'**AI predittiva** migliora la gestione dell'inventario, **prevedendo la domanda** dei prodotti e riducendo sprechi e costi operativi. Analizzando i comportamenti d'acquisto, tramite i dati raccolti non solo dalle carte fedeltà ma anche dai social, l'intelligenza digitale permette di personalizzare ulteriormente l'esperienza del cliente, aumentando la soddisfazione e le probabilità di acquisto. Anche il servizio clienti sarà più personalizzato: la nuova frontiera sono infatti **chatbot emotivamente intelligenti**, ovvero che sanno esprimere empatia basandosi su algoritmi di machine learning che analizzano le parole utilizzate dai clienti, il tono della loro voce e il contesto delle conversazioni.

LOGISTICA: EFFICIENZA OPERATIVA E RIDUZIONE DEGLI SPRECHI

La **logistica** può beneficiare ampiamente dell'AI generativa e dell'AI predittiva per **ottimizzare processi chiave** come la pianificazione dei percorsi di consegna e la gestione dei magazzini.
L'**AI generativa** analizza **variabili in tempo reale**, come traffico e condizioni meteorologiche, per generare percorsi ottimali.
L'intelligenza artificiale può anche tracciare il modo in cui i conducenti guidano i veicoli, individuano abitudini che sprecano carburante, come frenate brusche o velocità eccessiva. I conducenti possono essere quindi istruiti per avere consumi più contenuti.
La **manutenzione predittiva** riduce i costi di riparazione e i tempi di fermo dei veicoli. Aumenta anche la sicurezza rilevando i problemi in anticipo. Alcuni sistemi di intelligenza artificiale possono persino ordinare automaticamente i pezzi quando necessario.
Nel comparto della logistica del freddo, il ricorso a strumenti avanzati per il **controllo della temperatura e la tracciabilità** delle merci basati su AI è una priorità strategica. Questi sistemi non solo garantiscono il rispetto delle normative sulla conservazione dei prodotti, ma contribuiscono anche a ridurre gli sprechi.



Infine, la rapida crescita dell'**e-commerce** è destinata a incrementare la domanda di soluzioni innovative per la gestione dell'ultimo miglio. In tal senso, l'adozione di piattaforme basate sull'AI predittiva, combinate con veicoli autonomi e droni, promette di ridurre significativamente i **tempi di consegna e di ottimizzare l'allocazione** delle risorse.
Non è un percorso privo di sfide, ma con una pianificazione attenta e un approccio orientato all'innovazione, l'AI generativa e l'AI predittiva possono trasformare radicalmente i modelli di lavoro e i processi di qualsiasi realtà in qualsiasi settore, rendendola più proattiva, efficiente e in grado di rispondere alle mutevoli esigenze di un mercato in continua evoluzione.

LA **FORMAZIONE** ESSENZIALE PER FAVORIRE L'APPROCCIO **DATA-DRIVEN**

Combinare formazione, consapevolezza e strumenti tecnologici: è questa la ricetta che propone Alberto Vassena, CEO di Easynet Group per vincere la resistenza al cambiamento che è la principale sfida all'impiego dei dati come risorsa strategica per il successo aziendale

DI FABRIZIO PINCELLI

Una combinazione di attività straordinarie e iniziative di sviluppo endogeno sono alla base del percorso di crescita che sta attuando il provider di servizi gestiti **Easynet Group**. Un ruolo cruciale in tale percorso lo ricoprono i data analytics e le piattaforme di business intelligence, che l'azienda utilizza sia internamente sia come implementatore per altre realtà. *"Questo doppio ruolo ci permette non solo di migliorare la nostra operatività, ma anche di offrire soluzioni tecnologiche di valore ai clienti basate sulla nostra esperienza, contribuendo a creare una cultura aziendale data-driven"*. Lo afferma **Alberto Vassena, CEO di Easynet Group**, al quale abbiamo posto alcune domande per approfondire il tema del valore dei dati per il business.

D COME INTEGRATE I DATI NELLE DECISIONI QUOTIDIANE?

Utilizziamo strumenti avanzati di analisi dati per supportare ogni dipartimento aziendale. La reportistica settimanale, per esempio, include indicatori chiave come opportunità di vendita, percentuali di chiusura e previsioni di fatturato. Tali dati sono poi confrontati mensilmente per un'analisi più ampia. Questo approccio garantisce una visione chiara, strutturata e basata su elementi oggettivi, sia per la gestione interna sia per le strategie di mercato.
Un interessante esempio dell'adozione di tale approccio arriva da una media impresa italiana che, con il nostro supporto, ha adottato una piattaforma di business analytics. Inizialmente, tale azienda era orientata alla produzione, ma ha riconvertito il suo modello verso la rivendita, implementando un sistema per monitorare variabili complesse come logistica, fluttuazioni geopolitiche e prezzi delle materie prime. Prima dell'adozione della nuova piattaforma, le scelte venivano effettuate sulla base delle intuizioni e dell'esperienza dell'imprenditore. Con l'adozione della **business analytics**, completata in pochi mesi, l'azienda ha ottenuto un sistema che fornisce dati aggiornati quotidianamente. Questo ha permesso di supportare la crescita del business giunta in pochi anni da 30 a 70 milioni di ricavi annui.

D RECENTEMENTE HA PARTECIPATO A UN EVENTO RIVOLTO AGLI STUDENTI. QUAL È STATO IL SUO MESSAGGIO?

Ho tenuto uno speech presso l'Istituto Maria Ausiliatrice di Lecco dove ho sottolineato l'importanza del dato come risorsa strategica per il successo aziendale. Essere data-driven significa prendere decisioni più efficaci perché basate su numeri e analisi oggettive, non su intuizioni. Ho condiviso come questo approccio ci abbia permesso di crescere e di affrontare con successo sfide complesse, con l'intento di indurre i giovani a considerare il valore della gestione dei dati nel loro futuro professionale.

D QUALI SONO LE SFIDE PRINCIPALI ALLA DIFFUSIONE DI UNA CULTURA DATA-DRIVEN NELLE IMPRESE?

Una delle maggiori sfide è la **resistenza al cambiamento**, soprattutto nei contesti meno tecnologicamente avanzati. In Italia, il concetto di Industria 4.0 è stato spesso ridotto alla interconnessione macchinari – sistema informativo. Tuttavia, nei casi virtuosi, l'analisi di grandi quantità di dati ha permesso di fare scelte più ponderate, superando il limite delle intuizioni personali. La chiave è combinare formazione, consapevolezza e strumenti tecnologici adatti.

D AVETE LANCIATO UN'ACADEMY. COME SI DIFFERENZIA DAI PERCORSI FORMATIVI TRADIZIONALI?

La nostra Academy è nata per fornire competenze pratiche e professionalizzanti, adattate alle esigenze del nostro settore tecnologico. È una formazione che prepara giovani professionisti e figure senior ad affrontare le sfide tecnologiche contemporanee. Collaboriamo, infatti, con aziende partner e istituzioni accademiche per garantire una **preparazione concreta e direttamente applicabile** al mercato del lavoro. Uno dei punti di forza dell'Academy è il tasso di occupazione dei partecipanti: **la totalità trova lavoro**. Questo risultato deriva da un approccio formativo che combina teoria e pratica, offrendo l'opportunità di applicare subito le competenze acquisite. È un modello che valorizza l'integrazione tra apprendimento e realtà aziendale.

D IN QUALI SETTORI TROVANO APPLICAZIONE I VOSTRI PERCORSI FORMATIVI?

I programmi coprono ambiti fondamentali come la **sicurezza informatica**, il **cloud computing** e la **gestione delle reti**. Offriamo percorsi sia per giovani alle prime esperienze sia per professionisti già operativi. Questa diversificazione ci permette di rispondere alle esigenze di un mercato in continua evoluzione, con un focus sull'innovazione tecnologica.

A partire da marzo, lanceremo una serie di nuovi corsi all'interno dell'Academy. Non intendiamo prendere il posto dei percorsi universitari o di studio tradizionali, ma offrire un'alternativa complementare che valorizzi la formazione pratica e professionalizzante. I corsi rappresenteranno un percorso formativo innovativo e avranno una durata inferiore all'anno. Si tratta, infatti, di **percorsi intensivi e mirati**, che prepareranno sia all'ingresso nel nostro gruppo sia nelle aziende partner che operano all'interno del nostro ecosistema.

Questo modello formativo, unito alla capacità di implementare tecnologie analitiche avanzate, posiziona la nostra organizzazione come un partner chiave per aziende che vogliono affrontare le sfide del mercato con soluzioni innovative e basate su metriche oggettive.

ALBERTO VASSENA
CEO DI EASYNET GROUP

INTERNET OF THINGS CRESCE CON L'AI

L'AVVENTO DELL'INTELLIGENZA ARTIFICIALE STA FORNENDO ULTERIORE SPINTA ALLA DIFFUSIONE DI SOLUZIONI IOT, PREPARANDO IL TERRENO A UNA NUOVA RIVOLUZIONE TECNOLOGICA

DI MAURIZIO FERRARI

L'Internet of Things (IoT) è stata un'evoluzione tecnologica dirompente che, nel giro di pochi anni, ha modificato le infrastrutture IT ampliandone il perimetro d'influenza e trasformando per sempre le interazioni "uomo-macchina".
Oggi, con l'**avvento dell'AI**, siamo di fronte a una nuova rivoluzione in cui l'IoT diventa una delle **principali fonti di dati** per i sistemi di intelligenza artificiale sempre più esigenti. Oggi i sensori installati nelle macchine in produzione, nelle telecamere di sorveglianza e in molti altri dispositivi, come le automobili, sono una fonte inesauribile di dati che, grazie alle attuali soluzioni AI, possono diventare ancora più importanti nell'economia di un'azienda o per la pubblica amministrazione.

MERCATO SENZA CONFINI

Gli algoritmi di **machine learning, deep learning e analisi predittiva**, utilizzati dall'intelligenza artificiale, possono trasformare i dati grezzi ottenuti dall'IoT in **previsioni precise**, come la manutenzione predittiva, l'automazione avanzata e l'ottimizzazione operativa (per esempio, la gestione intelligente dell'energia). Dal punto di vista pratico è possibile fare alcuni esempi in ambiti che investono tutto il mercato, dal settore consumer a quello della pubblica amministrazione, del funzionamento di questa sinergia:

- **Smart Home:** i termostati intelligenti utilizzano l'AI per analizzare i dati di utilizzo e regolare la temperatura in modo ottimale.
- **Industria 4.0:** i macchinari connessi rilevano le anomalie tramite sensori IoT e prevengono i guasti prima che si verifichino grazie all'intelligenza artificiale.
- **Sanità:** dispositivi indossabili monitorano costantemente i parametri vitali e avvisano i medici in caso di anomalie.

IOT PER SISTEMI AUTONOMI

Questi esempi sono solo un assaggio di ciò che il connubio tra IoT e AI potrà fare in futuro, considerando gli sviluppi tecnologici delle infrastrutture IT. L'**edge computing** permetterà di analizzare i dati dei sensori IoT localmente, riducendo la latenza e garantendo maggiore sicurezza. In questo ambito si inserisce lo sviluppo di algoritmi AI più leggeri e ottimizzati. Un altro aspetto molto importante è **la sicurezza**: il connubio tra intelligenza artificiale e IoT può aiutare a sviluppare soluzioni per rilevare attacchi informatici e aumentare la protezione dei dati sensibili. Diventa quindi facile immaginare **ecosistemi completamente autonomi**, dove l'integrazione tra IoT e AI porterà alla creazione di ambienti in cui non sarà necessario l'intervento umano, come fabbriche automatizzate, città intelligenti e veicoli autonomi.
L'espansione delle **reti 5G e 6G** permetterà ai dispositivi IoT di diventare dei nodi di una **rete distribuita**, dove ogni dispositivo si farà carico di una parte dell'elaborazione, creando così architetture AI distribuite. Questo matrimonio può avere delle ripercussioni positive anche dal punto di vista della **sostenibilità ambientale**: le soluzioni IoT-AI permetteranno di **ottimizzare**

Con 5G e 6G, l'IoT diventa una rete distribuita con AI decentralizzata, ottimizzando risorse, efficienza energetica e riducendo le emissioni per una maggiore sostenibilità ambientale.

l'uso delle risorse naturali, migliorare l'efficienza energetica e ridurre le emissioni di carbonio. Naturalmente, non bisogna perdere di vista l'aspetto normativo di questa evoluzione per garantire che i dati IoT siano gestiti in modo etico e che gli algoritmi di AI siano equi e trasparenti.

Il **connubio tra IoT e AI** rappresenta un motore fondamentale per l'**innovazione tecnologica**. Con il progresso delle tecnologie di rete, dei sistemi di elaborazione e delle strategie di sicurezza, il loro impatto continuerà a crescere, trasformando il modo in cui viviamo e lavoriamo.

IoT: l'Italia vuole essere protagonista

Al CES 2025 di Las Vegas, le **start up italiane** hanno presentato **soluzioni IoT** concrete e sostenibili per il futuro delle città, delle industrie e della vita quotidiana. L'Internet of Things rappresenta uno dei **pilastri fondamentali** della trasformazione digitale a livello globale. Al CES 2025, l'Italia ha dimostrato di essere all'avanguardia, presentando 46 startup innovative che incarnano il meglio del "Made in Italy" tecnologico. La partecipazione era guidata dall'Agenzia ICE, che attraverso lo slogan *"Crafting innovation, shaping the future"* ha presentato l'Italia come un Paese in grado di combinare **creatività artigianale e tecnologie avanzate** per migliorare la qualità della vita e affrontare le sfide del futuro. Nell'arena tematica del padiglione italiano, aziende come ETIES, specializzata in sistemi IoT scalabili, e Liffo, innovatrice nel settore della cucina domestica automatizzata, hanno presentato soluzioni in grado di **rivoluzionare interi settori produttivi**. Inoltre, il progetto AIDA del Politecnico di Milano ha presentato la Maserati MC20 Cielo, dimostrando il ruolo cruciale delle tecnologie IoT per la **mobilità autonoma del futuro**.

IOT PER CITTÀ E INDUSTRIE INTELLIGENTI

Tra le **tecnologie presentate**, spiccano le soluzioni IoT per la **gestione intelligente dei rifiuti, la manutenzione predittiva e la sensoristica avanzata** per il monitoraggio ambientale. In questo contesto, il settore clean-tech ha avuto un ruolo di primo piano, presentando sistemi in grado di ridurre i **costi energetici industriali**

LE SOLUZIONI IOT RIVOLUZIONANO IL CLEAN-TECH: GESTIONE SMART DEI RIFIUTI, MANUTENZIONE PREDITTIVA E SENSORISTICA AVANZATA PER TAGLIARE I COSTI SENZA CAMBIARE MACCHINARI.

senza sostituire i macchinari esistenti. Un esempio emblematico è rappresentato dalla startup Blue Gold, che è stata premiata per l'**efficienza idrica** dei suoi dispositivi IoT integrati con intelligenza artificiale.
Le città del futuro saranno sempre più smart grazie all'IoT: dai sensori per il monitoraggio della qualità dell'aria e la prevenzione degli incendi a **soluzioni per la mobilità intelligente**, come robotaxi modulabili e supercondensatori per veicoli elettrici ad alte prestazioni. Anche il turismo e l'intrattenimento hanno beneficiato di tecnologie IoT innovative, con applicazioni che spaziano dai "concierge virtuali" per l'hospitality ai robot guida per musei.

TRA SFIDE E OPPORTUNITÀ

L'Italia ha dimostrato di possedere un **ecosistema imprenditoriale ricco di potenzialità**. Tuttavia, come evidenziato dall'Ey Venture Capital Barometer 2024, il settore del venture capital

italiano fatica a crescere rapidamente quanto i competitor europei. Con investimenti pari allo 0,06% del PIL, l'Italia si posiziona **al di sotto della media europea**, nonostante una crescita del 7,5% rispetto al 2023. I settori Health & Life Science, Software & Digital Services, **Technology & IoT**, Fintech ed Energy & Recycling sono i principali driver di sviluppo, con la Lombardia che svolge un ruolo di **traino per l'intero Paese**. L'IoT si conferma una tecnologia fondamentale per la sostenibilità. Soluzioni come quelle di Snelix, una startup che prova a **rivoluzionare l'elicicoltura con il vertical farming automatizzato**, dimostrano come l'IoT possa essere applicato a settori inaspettati per creare modelli produttivi innovativi e a basso impatto ambientale. Grazie al suo sistema modulare e brevettato, Snelix può monitorare e ottimizzare le condizioni ambientali delle sue farm, rispondendo concretamente alla crescente domanda di proteine alternative.
Il CES 2025 è stato per l'Italia non solo un **palcoscenico di visibilità internazionale**, ma anche un'opportunità per consolidare il ruolo delle sue start up nell'ecosistema globale dell'innovazione. L'IoT sta trasformando il nostro mondo e le startup italiane stanno dimostrando di essere pronte a cogliere questa trasformazione.

IOT E SICUREZZA

La sicurezza rimane una delle **principali preoccupazioni** quando si adottano soluzioni IoT in azienda. I dispositivi IoT, essendo connessi in rete, presentano diversi **punti deboli** che li rendono vulnerabili agli attacchi informatici. Molti dispositivi IoT hanno risorse **hardware e software limitate**, il che rende difficile implementare adeguate misure di sicurezza; inoltre, i produttori non rilasciano patch di sicurezza per correggere le vulnerabilità in modo tempestivo. Gli amministratori di sistema dovrebbero cambiare tutte le password predefinite di controllo, spesso reperibili nel dark web e potenzialmente compromesse. Se non adeguatamente protetti, i dispositivi IoT possono diventare facili bersagli per la creazione di botnet che possono essere usate per lanciare attacchi DDoS. Manca, inoltre, uno standard universale per la sicurezza dei dispositivi IoT, e la mancanza di interoperabilità tra sistemi e protocolli di comunicazione crea ulteriori punti deboli. Un'altra sfida per chi implementa queste soluzioni è la gestione e lo stoccaggio sicuro dei dati: i dispositivi IoT possono raccogliere grandi quantità di dati personali e sensibili degli utenti che devono essere protetti per evitarne l'uso illecito.

LE AZIONI NECESSARIE PER PROTEGGERE L'ECOSISTEMA IOT

- **implementare** standard di sicurezza più rigorosi per i dispositivi IoT;
- **garantire** aggiornamenti regolari e tempestivi per correggere le vulnerabilità;
- **adottare** tecnologie di crittografia e autenticazione avanzate;
- **sensibilizzare** gli utenti sull'importanza della sicurezza IoT.

INTERNET OF THINGS: UN MERCATO TRILIONARIO

L'**Internet of Things**, in concerto con l'**intelligenza artificiale**, con la sempre maggiore diffusione di infrastrutture a banda larga e 5G, e la crescente attenzione alla sostenibilità, stanno **trasformando il nostro modo di vivere e lavorare.** Questa tecnologia è destinata a raggiungere un **valore di mercato di 1,05 trilioni di dollari** nel 2025.

IOT IN CONTINUA CRESCITA

Dal 2018, l'IoT ha registrato una **crescita straordinaria, raddoppiando il proprio valore** di mercato. Oggi, le sue applicazioni sono onnipresenti: dalle case intelligenti alle fabbriche automatizzate, fino ai sistemi di monitoraggio sanitario. Secondo Statista Market Insights, il settore ha mantenuto un **tasso di crescita annuale composto (CAGR) del 12%** dal 2021, con ricavi in aumento di circa **100 miliardi di dollari ogni anno.** A trainare questa crescita sono i **segmenti industriali e consumer dell'IoT**, che nel 2025 rappresenteranno rispettivamente 275 e 235 miliardi di dollari. Inoltre, il **settore automotive**, che è il secondo per dimensioni, è previsto in crescita del 9%, fino a raggiungere i 274 miliardi di dollari.

CONNESSIONI IN AUMENTO

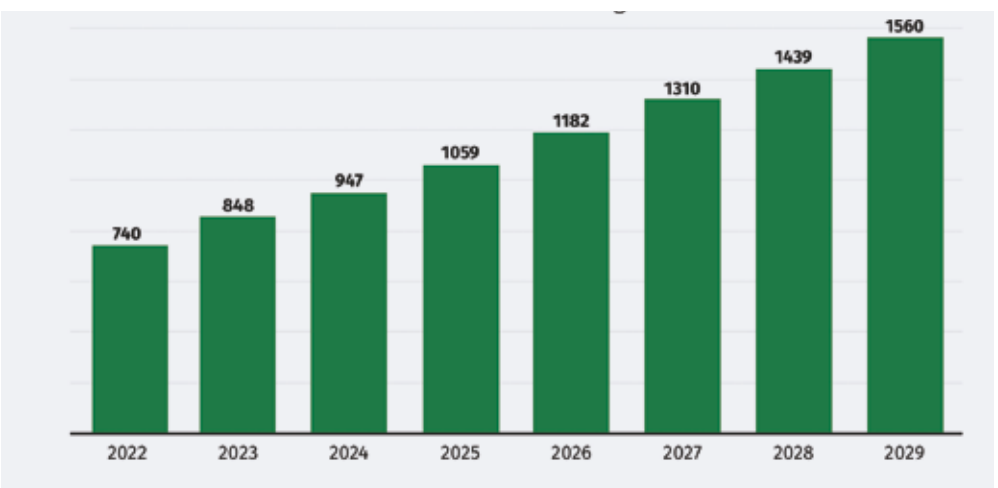
Il numero di **dispositivi connessi** continua a crescere a ritmi elevati. Nel 2021 si contavano 9,2 miliardi di connessioni IoT, mentre entro la fine del 2025 questo numero **salirà a 23,1 miliardi**, con una proiezione di quasi 40 miliardi entro il 2030. Questi dispositivi non solo migliorano l'efficienza operativa, ma forniscono anche **insight in tempo reale** che stanno rivoluzionando settori come la sanità, **l'agricoltura e la logistica**.

IL FUTURO

Con ricavi globali previsti in aumento di circa 120 miliardi di dollari all'anno, l'IoT potrebbe raggiungere un **valore di mercato di oltre 1.500 miliardi di dollari** entro il 2030. Questo traguardo evidenzia come l'Internet of Things non sia solo una **tecnologia del presente**, ma anche una **promessa per il futuro**, in grado di connettere persone, processi e dispositivi in modo mai visto prima d'ora.

Ricavi nel mercato mondiale IoT dal 2022 al 2029 (in miliardi di dollari USA)

Fonte: Statista Market Insights



5 TREND TECNOLOGICI CAMBIANO LA STRUTTURA DEI MERCATI

CAPGEMINI HA PRODOTTO LA TOP TECH TREND 2025 GLOBAL SURVEY SULLE PRINCIPALI TENDENZE TECNOLOGICHE. INEVITABILMENTE AI E GEN AI SONO LA BASE DI RIFERIMENTO CHE IN ALCUNI AMBITI STA GIÀ CAMBIANDO IN PROFONDITÀ CRITERI E ASPETTATIVE TRADIZIONALI. AD ESEMPIO? NELLA CYBERSECURITY, NELLA ROBOTICA E IN ALTRI SETTORI, ALLA RICERCA DI NUOVA PRODUTTIVITÀ, RESILIENZA E DI UN'INEVITABILE FLESSIBILITÀ PER FARE BUSINESS IN CONTESTI DOVE LA DISRUPTION È ORMAI UNA CONDIZIONE COMPETITIVA

DI STEFANO UBERTI FOPPA

Come da tradizione, arrivano tra gennaio e febbraio le previsioni sui principali trend tecnologici per l'anno in corso, considerando anche il loro potenziale impatto negli anni a venire dopo l'hype del momento. Ecco allora che anche **Capgemini** ha condotto nell'ottobre scorso la propria **Top Tech Trends 2025 Global Survey** su un campione di 1500 C-suite executive da dodici principali paesi tra Nord America, Europa e Asia-Pacific.

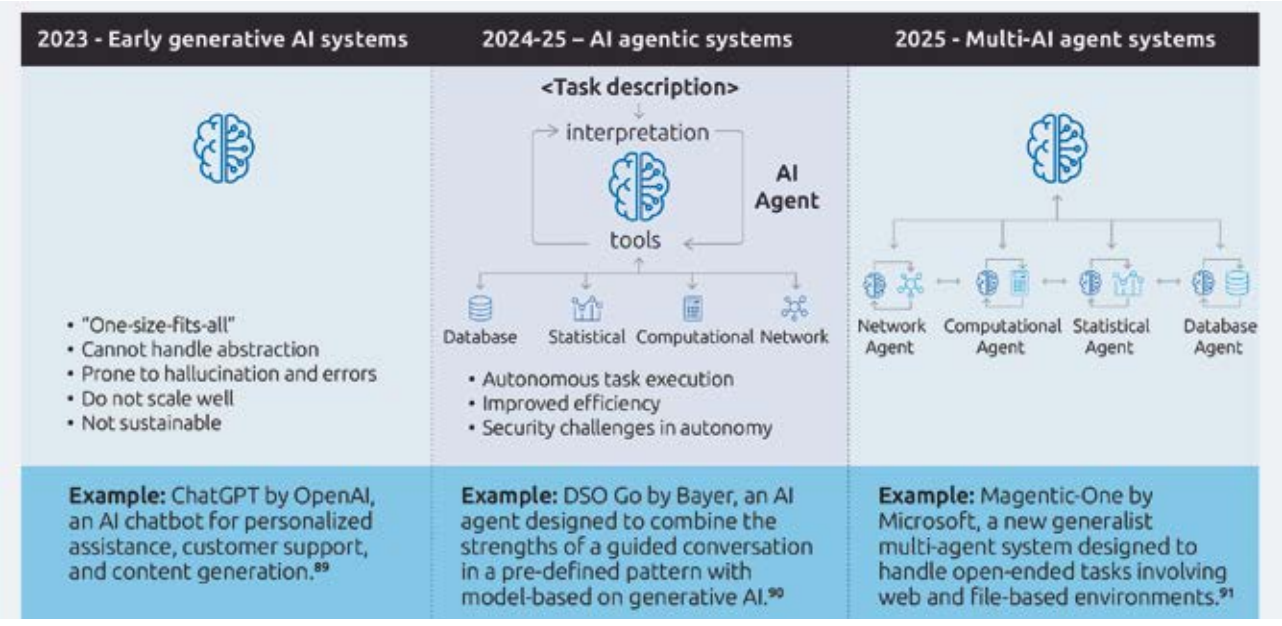
A questo campione di aziende, tutte con un fatturato annuale superiore al miliardo di dollari, ha aggiunto oltre 500 investitori professionali da venture capital, private equity e banche industriali oltre a interviste approfondite a 24 industry leader, analisti e accademici.

Inevitabilmente la base tecnologica non poteva che essere l'AI e la Gen AI, sempre più integrate in ogni tecnologia sia infrastrutturale sia applicativa. Ma è importante considerare che si tratta di soluzioni, secondo Capgemini, in grado di produrre non solo un miglioramento funzionale immediato, ma soprattutto un'evoluzione strutturale del segmento in cui verranno utilizzate. Queste tecnologie a base AI vengono declinate in **cinque macro ambiti**: **agenti software, cybersecurity, robotica, nuove tecnologie nucleari, supply chain.**

Guardiamole nel dettaglio.

DAI CO PILOT A "SUPER AGENTI" INTELLIGENTI CHE RAGIONANO E COORDINANO

Il concetto di autonomous, cioè la capacità dei sistemi informatici di apprendere, adattarsi alle situazioni e di conseguenza operare nel modo ottimale, si sta diffondendo nei diversi settori a risoluzione di specifici task (customer service, sanità, logistica, ecc). Il passo successivo, di cui si vedranno quest'anno le prime implementazioni, sarà la diffusione di **"super agenti"** capaci di orchestrare e ottimizzare differenti sistemi di AI. Queste tecnologie contribuiranno alla nascita di nuovi ecosistemi di AI nei diversi segmenti merceologici, aumentando l'efficienza e accelerando il tasso di innovazione delle imprese. Siamo in quella che Capgemini definisce "l'alba dell'agentificazione" in cui si passa da singoli agenti intelligenti focalizzati su specifici task a sistemi specializzati in grado di garantire un'**orchestrazione tecnologica** di agenti intelligenti e una governance di task complessi (ricerca autonoma di informazioni, gestione autonomous degli ordini, relazioni con i clienti, ecc.). La previsione si basa su due elementi: il primo è che alcuni top player, tipo Salesforce, Microsoft, Oracle, stanno proponendo framework multi agent, spesso open source, proprio nella funzione di meta-agent orchestratori. Il secondo elemento riguarda le previsioni di mercato. Una recente ricerca sempre di Capgemini sulla Gen AI ha sottolineato che ben l'82% delle aziende nel mondo prevedono di integrare nei propri sistemi IT agenti software nei prossimi 1-3 anni, per aumentare il livello di automazione e di capacità decisionale autonoma. Il mercato degli agenti AI è stato stimato nel 2024 da Capgemini attorno ai 5.1 miliardi di dollari, con una prospettiva di crescita ai 47.1 miliardi di dollari nel 2030 (tasso annuo medio di crescita del 44.8%).

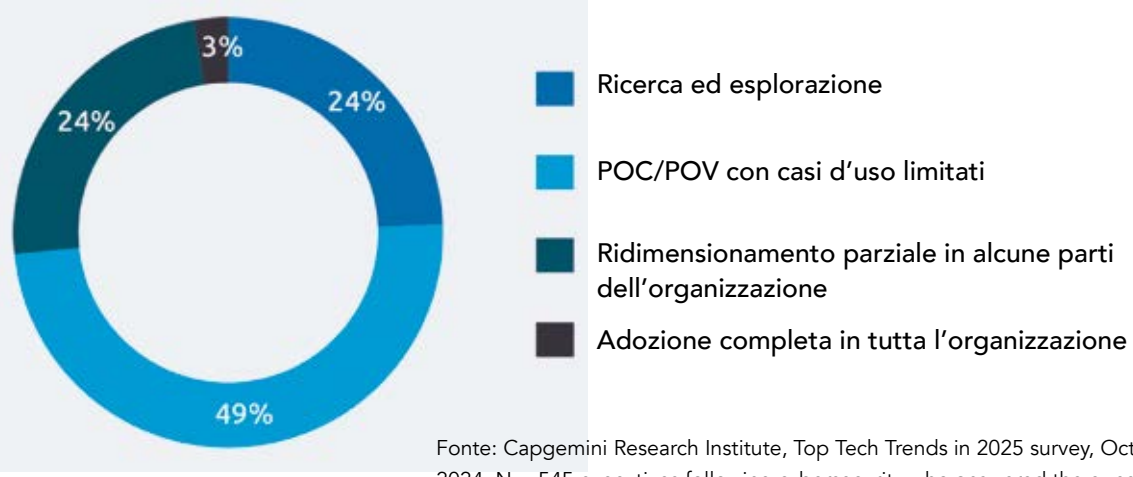


Fonte: Capgemini Research Institute analysis, Capgemini Applied Innovation Exchange – San Francisco

AI E GEN AI IN CYBERSECURITY: NUOVI LIVELLI DI DIFESA MA ANCHE DI ATTACCO

Il tema della vulnerabilità dei sistemi informativi è ormai una condizione strutturale per competere in mercati dove la digitalizzazione è parte integrante dei modelli di business. Era inevitabile quindi che la diffusione delle tecnologie di AI e Gen AI impattasse anche l'area della cybersecurity. Con queste tecnologie aumentano di sofisticatezza sia i livelli di protezione sia di attacco. Si parte da un dato importante: ben **il 97% delle organizzazioni** censite dalla ricerca hanno dichiarato di aver **subìto attacchi o problemi di sicurezza** attraverso l'utilizzo di AI e Gen AI negli ultimi anni (phishing sofisticato, ransomware, deepfake, nuovi schemi e modelli di frodi, ecc). Le imprese, cita il rapporto, hanno una sempre maggiore superficie informativa attaccabile, con nuove tecnologie esposte a una potenziale moltitudine di vulnerabilità. Questo anche perché se da un lato la "democratizzazione" nell'uso di tecnologie consentito dai tool di AI e Gen AI accelera i processi di ottimizzazione e performance, dall'altro consente anche a piccoli gruppi criminali di tentare operazioni di attacco su larga scala pur non disponendo delle competenze tecnologiche necessarie. È importante quindi predisporre framework orientati alla sicurezza IT che abbiano non solo una funzione di rilevazione delle vulnerabilità ma che, sfruttando l'autoapprendimento dell'AI e nuove capacità di orchestrazione sia di tecnologie sia di processi, possano indirizzarsi anche alla risposta e alla prevenzione dei rischi seguendo modelli di proattività. Ancora una volta, la diffusione di framework multi agent che coordinano software agent specializzati in attività di protezione dal cybercrime sui diversi componenti dei sistemi informativi sarà uno dei fenomeni più rilevanti del 2025.

MATURITÀ ORGANIZZATIVA DELL'IMPLEMENTAZIONE DELL'AI GEN NEL CAMPO DELLA SICUREZZA INFORMATICA NEL 2025



Fonte: Capgemini Research Institute, Top Tech Trends in 2025 survey, October 2024, N = 545 executives following cybersecurity who answered the question.

ROBOTICA, UN NUOVO LIVELLO DI COLLABORAZIONE UOMO-MACCHINA

La robotica sta da anni innervandosi di tecnologie AI. Nei diversi settori, i co-bot (collaborative robot) e una robotica basata su AI supportano l'attività umana in lavori di precisione nonché di elevato rischio. Lo sviluppo di Gen AI sta spingendo oggi alla creazione di nuovi sistemi "umanoidi" in grado di adattarsi di continuo alle diverse situazioni operative attraverso l'apprendimento costante del contesto in cui lavorano.
La prospettiva, con forti implicazioni di carattere organizzativo, culturale e professionale, è che con l'aumento dell'autonomia operativa di questi robot intelligenti, nonché con il loro utilizzo in ruoli e funzioni in cui sono in grado di prendere decisioni complesse, potrebbero sorgere problemi di ridefinizione dei criteri di gerarchia del lavoro tra esseri umani e robot. Una robotizzazione quindi che sta lasciando la dimensione di automazione di base per entrare in un territorio decisionale dove gli elementi da considerare, in un nuovo rapporto con l'essere umano, dovrebbero estendersi oltre la semplice ricerca di produttività.
Si tratta di previsioni suffragate dall'andamento dei dati negli ultimi anni: il mercato della robotica prevede infatti crescite significative guidate dall'**automazione industriale** sempre più spinta, carenza di lavoratori/competenze specialistiche, necessità di intervenire nella riduzione dei rischi e dei lavoratori umani. Le stime indicano che il mercato dei robot collaborativi sia stato di circa 2,3 miliardi di dollari nel 2024 con previsioni di 10,4 miliardi di dollari nel 2035. Il tasso medio annuo di crescita per il mercato globale dei robot umanoidi è previsto essere di circa il 154% dal 2024 al 2027, sostenuto da sempre maggiori investimenti da parte del mercato statunitense e cinese. Restano tuttavia aperti alcuni problemi: per lavorare efficacemente con i robot, le aziende devono investire nella **formazione e riqualificazione** dei propri dipendenti. Esiste poi un'oggettiva complessità legata all'integrazione tra queste soluzioni AI di elevato livello tecnologico e i sistemi esistenti nelle imprese (il 43% degli executive dichiara un'infrastruttura IT inadeguata). Da non sottovalutare infine i problemi legati a normative del lavoro e security/qualità. Per questi ultimi, ad esempio, senza dataset estesi, ben mantenuti e protocolli di raccolta dati adeguati, i sistemi di intelligenza artificiale possono produrre output inaccurati e/o distorti (dovuti ad esempio a bias, in questo caso l'istruzione dei dati di training o dell'algoritmo di AI condizionata da una serie pregiudizi, anche involontari, umani), portando a sprechi e problemi di qualità negli ambienti di produzione.

PREVISIONE DEL LIVELLO DI ADOZIONE DEI ROBOT AI-BASED NEL 2025

Fonte: Capgemini Research Institute, Top Tech Trends in 2025 survey, October 2024

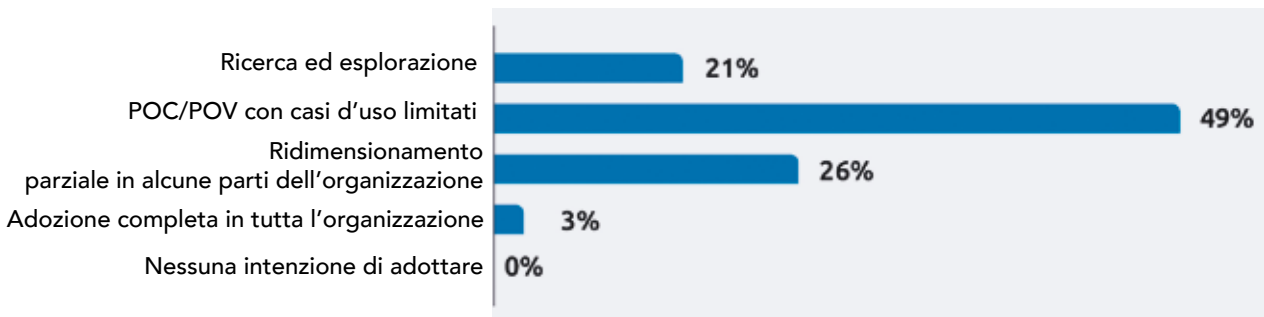
L'AI AUMENTA LA RICHIESTA DI ENERGIA: CRESCE L'INTERESSE PER IL NUOVO NUCLEARE

Quello di una rinascita dell'energia nucleare prodotta attraverso sistemi più sicuri, economici, controllabili, con piccoli reattori modulari, è un tema che possiamo considerare dalla sola prospettiva tecnologica. Troppe sono infatti le implicazioni culturali, politiche, ambientali, persino emotive, collegate. Il report tuttavia rileva che la necessità di energia pulita per rispondere alle esigenze di innovazione in tutti i settori secondo logiche di sostenibilità sta trasformando a un ritmo senza precedenti il comparto energetico. L'**Energy Outlook 2023** della Energy Information Administration (EIA) americana prevede che la domanda globale di energia prodotta da **tecnologie zero carbon** (comprese quella nucleare) aumenterà tra il 30 e il 76% dal 2050. Crisi climatica e domanda "energivora" legata all'innovazione tecnologica in tutti i settori, stanno guidando la ricerca e gli investimenti nelle rinnovabili, dai biocarburanti all'idrogeno a basse emissioni di carbonio e oltre. L'**energia nucleare** emerge dal report come uno dei punti di attenzione per il 2025 (l'anno scorso non era nemmeno considerata), essendo stata spinta in cima al ranking dall'urgente necessità di nuova energia pulita anche per rispondere all'**enorme domanda di energia richiesta dall'intelligenza artificiale** e in genere da una sempre più capillare digitalizzazione della società e dei mercati. Google, Meta, Amazon, Oracle sono solo alcuni dei nomi che a causa della forte domanda mondiale di servizi cloud e di tecnologie AI e AI Gen, con i relativi data center sempre crescenti in potenza di calcolo necessaria, hanno registrato livelli di emissione di carbonio in costante aumento negli ultimi anni. Questi grandi player IT sono oggi direttamente (attraverso accordi per partecipare a progetti per lo sviluppo di impianti di nuova energia nucleare) o indirettamente (annunci di acquisto di energia da impianti nucleari di nuova generazione di terzi) coinvolti nello sviluppo di SMR (Small modular reactors), reattori modulari di nuova generazione a fissione nucleare di piccola taglia (della dimensione di container) installando le diverse unità laddove esista l'esigenza di alto consumo energetico.

SUPPLY CHAIN DI NUOVA GENERAZIONE: AGILI, SOSTENIBILI E SUPPORTATE DALL'AI

Se c'è un settore che da sempre sperimenta per primo soluzioni IT innovative, quello è la logistica, la **supply chain**. Negli ultimi anni blockchain, analytics real time, IoT diffusa per tracking e security e ora, tecnologie di AI e Gen AI rappresentano soluzioni per muoversi nella complessità attuale dei mercati. Le fibrillazioni geopolitiche da sempre impattano le catene di approvvigionamento, ma certo la continua "disruption" sperimentata in questi ultimi anni, le tensioni commerciali Usa-Cina-Europa, la guerra Russia-Ucraina, l'epidemia Covid 19, l'instabilità continua nel medio-oriente, spinge le imprese a ricercare una maggiore flessibilità e resilienza delle proprie supply chain, diversificando le location, riducendo le dipendenze dalle singole regioni geografiche, sviluppando una capacità di ridisegnare con rapidità i flussi di approvvigionamento.
La nuova generazione di supply chain, sempre più guidata dall'analisi in real time dei dati e con il supporto operativo, proattivo e autonomous dell'AI, focalizza almeno sette diverse aree: demand forecasting e planning; supply e procurement management; smart manufacturing (predictive maintenance, automation, ecc); warehouse e transportation automation; sustainability e circular supply chain; risk e disruption; abilitazione/supporto alla forza lavoro. Circa il 70% tra i 1.550 executive dell'indagine indica proprio questa **supply chain "AI based"** come il **maggiore trend tecnologico** per il 2025 e attualmente il 49% delle organizzazioni si trova già nella fase PoC su alcune aree. Il 2025, prevede quindi Capgemini, sarà di prova per queste tecnologie che raggiungeranno un nuovo livello di automazione. Tuttavia, per i prossimi anni, cita lo studio, *"Ci aspettiamo una vera rivoluzione nelle supply chain: non solo diventeranno sempre più intelligenti ma anche spettacolari, in grado di armonizzare velocità, trasparenza e resilienza nei diversi contesti industriali"*.

LIVELLO DI ADOZIONE PREVISTO DALLE ORGANIZZAZIONI NEL 2025:
"SUPPLY CHAIN DI NUOVA GENERAZIONE"



Fonte: Capgemini Research Institute, Top Tech Trends survey; October 2024, N = 1,500 Executives, and N = 500 VCs (Investors), N = 603 Executives following industry & engineering domain, new-generation supply chains selected among top three ranks N = 425 executives who answered the question.

LA RIVOLUZIONE DIGITALE DELLA **FINANZA** E DEI **SERVIZI BANCARI**

NON SOLO COMPLIANCE ALLE NORMATIVE, MA ANCHE SERVIZI INNOVATIVI DI PAGAMENTO, GESTIONE "INTELLIGENTE" DEL CLIENTE, CLOUD, SICUREZZA E METAVERSO: IN UNO SCENARIO SEMPRE PIÙ DEMATERIALIZZATO SI STA RIDEFINENDO IL MODELLO FINANZIARIO E LA RELAZIONE COL CLIENTE

DI FABRIZIO PINCELLI

Da sempre, il settore finanziario e dei servizi bancari è uno di quelli che mostra le maggiori resistenze riguardo le innovazioni e le trasformazioni. Tuttavia, va da sé che sia anche tra i più attenti all'efficienza e al risparmio sui costi. Così, dopo avere valutato con attenzione l'evoluzione delle tecnologie IT, e spinto anche dalla necessità di aderenza alle normative, sta puntando in maniera sempre più pervasiva sulla trasformazione digitale. Questo sta portando a una ridefinizione dei modelli operativi, dei servizi offerti e del rapporto con i clienti. Dalla gestione avanzata del cliente basata sull'intelligenza artificiale (AI) alle soluzioni di pagamento innovative, dall'adozione del cloud computing alla sicurezza informatica, fino all'emergente potenziale del metaverso, la finanza sta percorrendo la strada verso un futuro sempre più dematerializzato.

COMPLIANCE NORMATIVA E TRASFORMAZIONE DIGITALE

La crescente complessità delle normative che a livello globale caratterizza il settore richiede strumenti più sofisticati di quelli usati tradizionalmente per garantire l'aderenza in tempo reale, al fine di migliorare la trasparenza e ridurre il rischio di sanzioni. In tale contesto, la compliance normativa è una delle principali aree in cui le tecnologie IT stanno dimostrando il loro valore. In particolare, le **piattaforme di RegTech** (Regulatory Technology) hanno letteralmente rivoluzionato la gestione della compliance. Basate su algoritmi avanzati e intelligenza artificiale, tali piattaforme includono strumenti come software di analisi dei dati, sistemi di monitoraggio e di reportistica. Questi permettono di tenere sotto controllo e analizzare grandi volumi di dati in modo automatico, identificando eventuali anomalie o violazioni. Il machine learning consente poi ai sistemi di apprendere dai dati storici, migliorando continuamente l'efficienza dei processi di conformità.

Inoltre, per analizzare documenti normativi e tradurli in azioni operative per le istituzioni finanziarie possono essere impiegate tecnologie come il **Natural language processing** (NLP) in modo da agire semplicemente attraverso comandi vocali.

Con particolare riferimento all'antiriciclaggio, la Banca d'Italia cita il ricorso alla **SupTech** (superior technology), ovvero strumenti avanzati di raccolta e analisi di dati eterogenei in modo da ottenere un importante risparmio di tempo e risorse. Si tratta di strumenti che usano tecniche quali *"network analysis, Natural language processing, text mining e machine learning per aumentare la capacità di individuare reti di transazioni, identificare comportamenti anomali e trasformare grandi quantità di dati, strutturati e non, in informazioni utili a fini operativi"*.

INNOVAZIONE NEI SERVIZI DI PAGAMENTO

I sistemi di pagamento stanno vivendo una trasformazione radicale, grazie all'introduzione di tecnologie come blockchain, mobile payment e sistemi contactless. La diffusione delle applicazioni fintech ha portato alla nascita di soluzioni come portafogli digitali, app di pagamento P2P (person to person) e valute digitali.

La blockchain, in particolare, rappresenta un cambio di paradigma. È contraddistinta da peculiarità quali elevata sicurezza, trasparenza e immutabilità. Questo le consente di abilitare transazioni in tempo reale senza la necessità di intermediari. Inoltre, forme di denaro puramente digitali come le **Central Bank Digital Currencies** promettono di integrare le funzionalità delle criptovalute nel sistema finanziario tradizionale. Secondo il più recente report dell'Atlantic Council, 134 paesi e unioni monetarie, che rappresentano il 98% del PIL globale, stanno esplorando una CBDC. Ogni paese del G20 sta esplorando una CBDC e 13 sono già nella fase pilota. Tra questi, Brasile, Giappone, India, Australia, Russia e Turchia.

L'evoluzione dei sistemi di pagamento non si limita però alla tecnologia blockchain. L'apertura a nuovi standard come quelli introdotti dalla **direttiva PSD2** (Payment Services Directive 2) in Europa ha aperto le porte all'open banking, consentendo a terze parti di sviluppare applicazioni e servizi che si integrano direttamente con i conti bancari dei clienti e aprono la via a nuove opportunità per l'innovazione.

L'INTELLIGENZA ARTIFICIALE ALLA BASE DEL RAPPORTO CON I CLIENTI

La customer experience è diventata il fulcro della strategia delle istituzioni finanziarie. Le operazioni allo sportello sono un lontano ricordo. Oggi, è l'intelligenza artificiale lo strumento basilare per personalizzare i servizi e migliorare l'interazione con i clienti.

I chatbot e gli assistenti virtuali, basati su tecnologie di **AI conversazionale**, sono ora in grado di gestire una vasta

SICUREZZA INFORMATICA, PRIORITÀ ASSOLUTA

Con l'aumento della digitalizzazione, la sicurezza informatica è diventata una delle principali preoccupazioni anche per il settore della finanza e dei servizi bancari. Gli attacchi informatici, come il phishing, il ransomware e le frodi online, rappresentano minacce significative non solo per gli operatori ma anche per i loro clienti.
Le tecnologie di cybersecurity basate su AI stanno rivoluzionando la difesa contro queste minacce. Strumenti di anomaly detection analizzano costantemente i dati delle transazioni per identificare comportamenti sospetti in tempo reale, riducendo il rischio di frodi.
Allestire oggi un sistema per la sicurezza informatica non è solo necessario per proteggere il business e clienti, ma anche obbligatorio per soddisfare precisi richieste imposte da norme come la direttiva NIS2 e DORA, oltre che dal GDPR.
Un altro aspetto da non sottovalutare sono i sistemi di autenticazione multifattoriale e biometrica: il loro impiego migliora ulteriormente la sicurezza dell'accesso ai servizi finanziari. Questo soprattutto a fronte della diffusione di deepfake vocali e video sempre più difficili da rilevare.

gamma di richieste, dalle operazioni bancarie di base alla consulenza finanziaria. Questi strumenti non solo migliorano l'efficienza operativa, ma offrono anche un servizio ininterrotto, 24/7. Inoltre, i comportamenti dei clienti sono analizzati tramite algoritmi di machine learning in modo da proporre prodotti finanziari su misura. L'obiettivo è aumentare il tasso di fidelizzazione.
Analogamente, attraverso le piattaforme di robo-advisory si possono fornire consulenze sugli investimenti evitando l'interazione con i consulenti. Tali piattaforme utilizzano l'AI per combinare dati storici e analisi in tempo reale al fine di suggerire strategie personalizzate, rendendo gli investimenti accessibili anche ai meno esperti.

CLOUD COMPUTING: SE IBRIDO, È UN'OTTIMA OPPORTUNITÀ

Il cloud computing è diventato un pilastro essenziale per la trasformazione digitale nel settore finanziario. L'adozione del cloud consente alle istituzioni di scalare rapidamente le loro operazioni, riducendo i costi infrastrutturali e migliorando la flessibilità. Inoltre, l'integrazione di soluzioni cloud native facilita l'implementazione di tecnologie avanzate come l'analisi predittiva e l'automazione.
Un aspetto critico nell'adozione del cloud è la sicurezza. I fornitori di servizi cloud stanno investendo significativamente in misure di protezione, come la crittografia avanzata e i sistemi di rilevamento delle intrusioni basati su AI. Tuttavia, l'adozione del

cloud comporta anche sfide legate alla conformità normativa e alla gestione dei dati, specialmente in un contesto internazionale in cui le regolamentazioni sulla privacy variano tra i diversi paesi e dove assume un ruolo essenziale la sovranità dei dati.
Proprio per questo con il termine cloud va inteso il **cloud ibrido**: istituti finanziari e banche non possono spostare tutte le loro attività tutte sul cloud. Molte operazioni devono essere eseguire ancora on premise, ma con infrastrutture che devono permettere di essere al passo con l'evoluzione tecnologica per poter operare in real time. Le banche stanno così adottando approcci ibridi (e anche multi-cloud) per bilanciare le esigenze di innovazione e conformità normativa.

VERSO UN MODELLO DEMATERIALIZZATO, MA RISPETTOSO DELL'AMBIENTE

Il crescente ricorso alle tecnologie IT sta accelerando la transizione verso un modello finanziario sempre più dematerializzato. Questo nuovo paradigma non solo riduce la dipendenza dalle infrastrutture fisiche, ma migliora anche l'efficienza operativa e l'accessibilità ai servizi finanziari.
Per esempio, la digitalizzazione dei processi documentali consente di eliminare la necessità di supporti cartacei, semplificando le operazioni e riducendo i costi. Allo stesso tempo, l'uso di strumenti digitali come le firme elettroniche e i contratti intelligenti (smart contract) sta migliorando la velocità e l'affidabilità delle transazioni.
Intelligenza artificiale, velocità e automazione richiedono però elevate performance e alti livelli di computing. Questo si traduce in rilevanti consumi energetici. Nasce così una sfida importante: coniugare le prestazioni con le sempre più pressanti richieste di sostenibilità e la necessità di promuovere **misure ESG**. Non va infatti scordato che dal 2025 sono obbligate a redigere il bilancio di sostenibilità (in relazione all'anno 2024) tutte le imprese quotate e di pubblico interesse con più di 500 persone e 25 milioni di euro di stato patrimoniale o 50 milioni di ricavi netti. Tale obbligo verrà gradualmente esteso a tutte le grandi imprese e a tutte le aziende quotate entro il 2029.

È IL METAVERSO LA NUOVA FRONTIERA DELLA FINANZA?

Di metaverso si parla da diversi anni, ma il mondo virtuale non è ancora decollato come molti invece si aspettavano. Tuttavia, per il settore finanziario rappresenta una delle opportunità più affascinanti. Infatti, grazie alle sue caratteristiche, questa nuova dimensione virtuale potrebbe rivoluzionare il modo in cui le istituzioni interagiscono con i clienti, offrendo esperienze immersive e personalizzate. Alcune banche stanno sperimentando la creazione di **filiali virtuali all'interno del metaverso**, dove i clienti possono incontrare consulenti finanziari e dialogare con loro tramite avatar, simulando quanto avviene nel mondo reale ma secondo una modalità molto più immersiva. Inoltre, la blockchain abilita la trasformazione in token di asset reali e digitali rendendolo così di nessun valore per i criminali informatici. Così si creano nuove opportunità per investimenti e scambi all'interno di tali ambienti virtuali.
Tuttavia, l'adozione del metaverso presenta anche sfide significative, come la necessità di sviluppare standard di interoperabilità, garantire la sicurezza delle transazioni e affrontare questioni legate alla privacy dei dati.
Più in generale, il settore finanziario e dei servizi bancari si trova all'avanguardia della trasformazione digitale, grazie all'integrazione di tecnologie IT avanzate. Questa evoluzione, tuttavia, non è priva di sfide. La necessità di bilanciare innovazione e sicurezza, garantire la privacy dei dati e adattarsi a un panorama normativo in continua evoluzione saranno elementi chiave per il successo futuro.

BICTA, LA PIATTAFORMA CHE RICONCILIA I **FLUSSI DI CASSA**

Una soluzione modulare che riconcilia automaticamente incassi e pagamenti, fornendo una visione finanziaria univoca, coerente e aggiornata in tempo reale per automatizzare azioni e favorire decisioni strategiche efficaci.

DI RICCARDO FLORIO

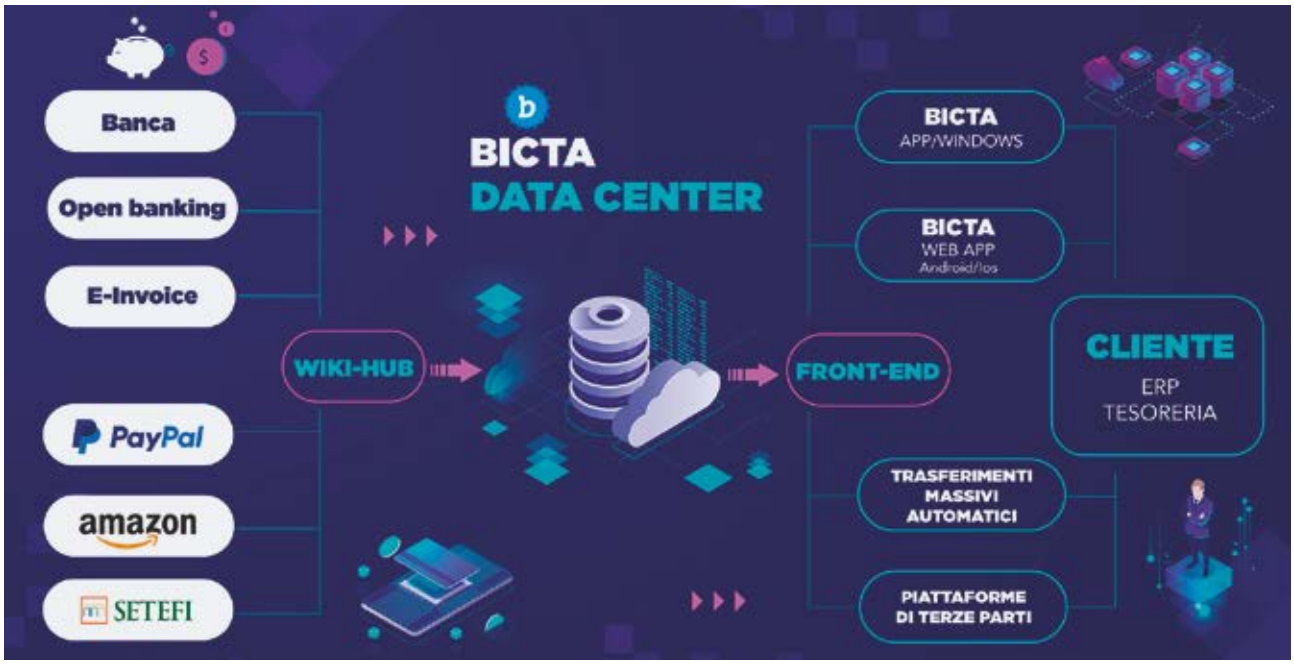
FRANCO FERIOLI ALESSIO,
COO DI WIKI SOFTWARE INTERNATIONAL

Da oltre 20 anni, Wiki Software International, azienda nata nel torinese e con sede in Svizzera, supporta CFO, direttori finanziari, controller, credit manager e treasury manager con strumenti tecnologici avanzati, pensati per fornire informazioni tempestive e dati in tempo reale sui flussi finanziari. Attraverso **la piattaforma Bicta**, Wiki Software mette a disposizione **una soluzione modulare che automatizza la riconciliazione di tutti gli incassi e i pagamenti**, garantendo una gestione efficiente e puntuale dei flussi finanziari. Ciò permette alle aziende di trasformare la gestione finanziaria in un asset strategico per migliorare le performance organizzative.

UNA SOLUZIONE CHE AGGIUNGE VALORE ALLA TESORERIA

"Siamo una software factory con una lunga e comprovata esperienza nel settore finanziario - spiega **Franco Ferioli Alessio, COO di Wiki Software International** - *e, nel corso degli anni, abbiamo progressivamente messo a frutto le nostre competenze specializzandoci in un ambito legato alla tesoreria. Oggi ci rivolgiamo ad aziende di ogni settore che devono gestire un elevato numero di fatture e/o clienti, offrendo loro una soluzione efficace per garantire una gestione puntuale di incassi e pagamenti."* Bicta non si sostituisce ai software di tesoreria tradizionali, ma li integra e ne amplifica le potenzialità senza richiedere modifiche infrastrutturali o creare problemi di compatibilità.

"I moduli di tesoreria base hanno come obiettivo quello di far quadrare i conti - continua Ferioli Alessio - *e sono focalizzate sulla gestione della informazioni*



acquisite senza intervenire sulle informazioni stesse. La nostra azione, invece, è rivolta a ottimizzare i flussi informativi, fornendo una soluzione che si affianchi ai software esistenti per garantire dati aggiornati in tempo reale e un'operatività più coerente ed efficace."
Bicta funge da sincronizzatore centralizzato per tutte le transazioni consentendo, per esempio, di impostare solleciti automatici all'immediata scadenza dei termini di pagamento e di gestire gli incassi in maniera fluida e senza errori. Il risultato porta a operazioni di controllo e verifica dei pagamenti accelerate, un più agevole recupero crediti e una riduzione degli errori contabili, con un impatto positivo generale sulla gestione della tesoreria.
Operando in modo automatico e non presidiato, la piattaforma aiuta CFO, direttori finanziari e tesorieri a **ottenere dati sempre aggiornati e accurati,** migliorando i processi decisionali e la gestione dei pagamenti.
"Più un'azienda cresce, più complessa diventa l'integrazione dei diversi sistemi di incasso - aggiunge il COO di Wiki Software -. *I nostri clienti sono realtà con un elevato volume di fatture e hanno anche il problema di mantenere invariato nel tempo l'accesso allo storico delle transazioni. Bicta crea un repository centralizzato al cui interno restano conservati in modo sicuro tutti i dati storici. Questi dati restano a disposizione per ogni esigenza di gestione e rappresentano un asset che resta all'interno dell'azienda, anche in caso in cui questa decida di cambiare la banca di appoggio."*

SINCRONIZZARE TUTTE LE MODALITÀ DI PAGAMENTO

Oggi assistiamo a un progressiva disintermediazione bancaria, con aziende che offrono strumenti di pagamento proprietari o integrati in App di terze parti. Questa evoluzione implica la necessità di un costante aggiornamento e integrazione con le nuove piattaforme di pagamento, affinché i sistemi aziendali di contabilità e tesoreria possano gestire in modo corretto i relativi flussi finanziari.
"Oggi è il cliente che decide come pagare e l'azienda deve adeguarsi – precisa Ferioli Alessio -. *Bicta permette di affrontare efficacemente il tema spinoso legato alla proliferazione dei sistemi di pagamenti che, non solo devono essere riconciliati, ma vanno anche mantenuti nel tempo. Attraverso il middleware WikiHUB viene* ***abilitata all'interno della piattaforma la sincronizzazione di tutte le modalità di pagamento, incasso e rendicontazione****: bancarie, Open Banking PSP, PayPal, Amazon, Setefi/Nexi, e-invoice SDI. Questo consente di* ***rendere immediatamente fruibile il servizio anche nei sistemi gestionali o nei siti Internet dei clienti.****"*
Tramite Bicta, le aziende possono, quindi, ridurre errori contabili, accelerare il recupero crediti e ottenere una visione finanziaria sempre aggiornata ottenendo un rapido ritorno dell'investimento.
Il software è disponibile in modalità di abbonamento e viene commercializzato sia direttamente sia tramite distributori autorizzati.

PROSPETTIVE
VERTICALI

Le nuove frontiere
del tech nei settori verticali

DORA È LEGGE. OPPORTUNITÀ E SFIDE PER IL **SETTORE FINANZIARIO**

Dal 17 gennaio 2025, il settore finanziario europeo affronta una trasformazione: DORA non è solo una normativa, ma un nuovo paradigma di resilienza operativa, che unisce innovazione, sicurezza e governance per affrontare le sfide digitali

Il 17 gennaio 2025 è una data che segna una svolta per il settore finanziario europeo. Con l'entrata in vigore del regolamento europeo Digital Operational Resilience Act (DORA), le istituzioni finanziarie dello spazio economico europeo e i loro fornitori di servizi ICT sono chiamati a un cambiamento epocale: costruire un'architettura digitale capace di resistere a eventi critici e garantire la continuità operativa. Il settore finanziario è spinto da crescenti aspettative per servizi in tempo reale e comunicazioni digitali multicanale, soprattutto dai millennials. Per ottimizzare costi e scalabilità e per sfruttare anche innovazioni come AI e Generative AI, le istituzioni adottano infrastrutture cloud di terze parti, ampliando però la superficie d'attacco cyber oltre i confini tradizionali.
A pochi giorni dall'entrata in vigore, DORA si conferma non solo un insieme di requisiti tecnici, ma un nuovo modello di resilienza operativa. La trasformazione digitale, da una lato offre nuove opportunità di business, dall'altro ha creato interdipendenze fra gli attori economici del mondo finanziario e fra questi e i loro fornitori ICT che amplificano il rischio sistemico nel settore finanziario. Questo regolamento affronta tali rischi per proteggere il sistema e i cittadini europei.

Un impatto trasversale e immediato

La normativa interessa direttamente oltre 20.000 entità finanziarie nell'Area Economica Europea (EEA), inclusi banche, assicurazioni e operatori dei mercati dei capitali, oltre ai fornitori critici di servizi ICT.
Per molti, però, la strada per la conformità appare ancora in salita. Secondo la European Security Technologies and Strategies Survey 2024 di IDC, condotta a maggio del 2024, quasi la metà degli intervistati (49%) dichiarava di non aver ancora intrapreso azioni significative per adeguarsi a DORA, mentre il 14% non era nemmeno a conoscenza della normativa. E in un'indagine IDC condotta a ottobre 2024 (IDC Financial Insights Survey 2024, October 2024) emerge che solo 1 istituzione finanziaria su 4 si dichiarava pronta per la conformità con i dettami regolamentari di DORA in merito al coinvolgimento della board room e alla chiara definizione dei ruoli e delle responsabilità, mentre solo un ulteriore 36% ha dichiarato che sarebbe stata compliant per la scadenza di gennaio 2025, quindi il 40% degli intervistati ha dichiarato che non sarebbe stato conforme per tempo. Questi dati evidenziano un'urgenza: non solo per colmare le lacune regolamentari, ma anche per costruire una strategia di resilienza che garantisca stabilità in un contesto economico sempre più complesso e digitalizzato.

Armonizzazione e supervisione: due principi chiave di DORA

Tra le innovazioni introdotte, DORA si distingue per la volontà di assicurarsi che i dettami regolamentari siano coerenti fra i vari Paesi e che la supervisione della conformità ricada tanto sulle istituzioni finanziare quanto sui fornitori ICT a supporto delle funzioni critiche. Portare direttamente questi attori, sinora non regolamentati, sotto la supervisione diretta delle autorità di vigilanza finanziare rappresenta un significativo cambiamento di paradigma. I due principi guida possono essere così sintetizzati:

- Armonizzazione regolamentare: Unifica i dettami regolamentari per oltre 20.000 imprese nell'EEA, e elimina discrepanze normative tra Stati membri grazie a un regolamento direttamente applicabile, semplificando il quadro normativo, per le imprese multinazionali.
- Supervisione diretta dei fornitori ICT: Per la prima volta, i fornitori critici, come quelli cloud, sono sottoposti alla supervisione delle autorità europee di vigilanza finanziaria (EBA, ESMA, EIOPA) per ridurre il rischio sistemico derivante dalla dipendenza tecnologica.

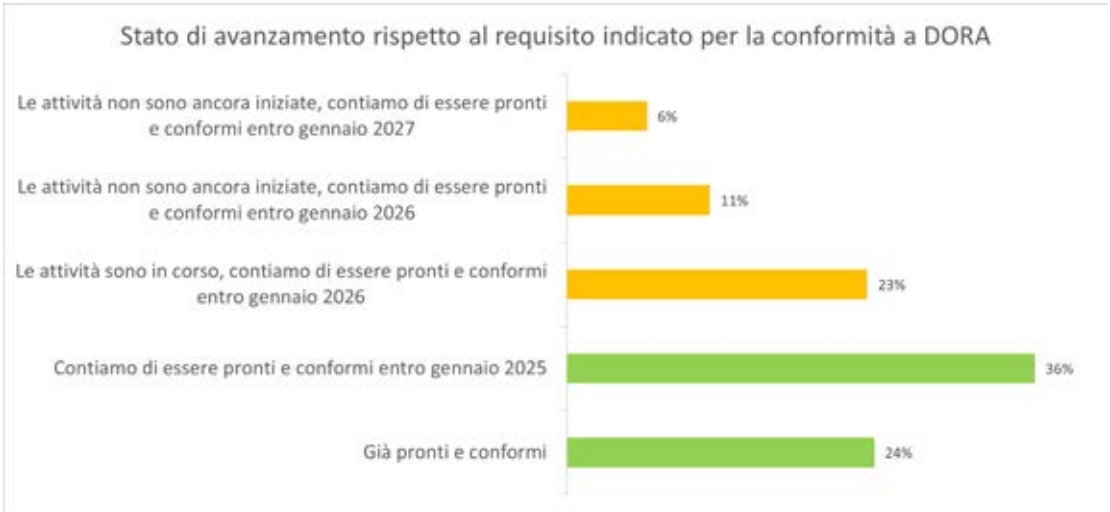
DORA prevede un framework per una collaborazione più stretta fra istituzioni finanziarie e i partner ICT, garantendo una robustezza operativa end-to-end. Per i partner ICT, DORA non rappresenta solo un nuovo onere normativo, ma un'opportunità per rafforzare le relazioni con i clienti ed esplorare nuove opportunità di business, poiché le istituzioni finanziarie devono condurre ricerche di mercato e individuare soluzioni alternative per ogni funzione critica.

Una sfida di governance e mercato

DORA impone alle istituzioni finanziarie una gestione più rigorosa del rischio operativo e della governance dei fornitori terzi. Per mitigare il rischio sistemico il regolamento europeo definisce 5 pilastri a cui ricondurre i vari requisiti di conformità

1. Gestione del rischio ICT
2. Gestione, classificazione e segnalazione obbligatorie degli incidenti legati all'ICT
3. Test di resilienza operativa digitale
4. Gestione del rischio ICT derivante da terze parti
5. Condivisione volontaria delle informazioni

Coinvolgimento della C-suite e chiara definizione di ruoli e responsabilità



IDC Survey 2024: Financial Insights Survey, October 2024. N=650

Inoltre, le istituzioni finanziarie devono definire strategie di uscita chiare per mitigare il rischio sistemico nel caso di problemi operativi con un partner ICT esistente, identificando e selezionando soluzioni e fornitori alternativi per garantire il trasferimento senza interruzioni dei servizi critici, ove necessario.
Molti dei requisiti di DORA non sono nuovi per le grandi istituzioni, in particolare per le banche significative soggette al Meccanismo di Vigilanza Unico (SSM) della BCE, ma rappresentano una novità per altri enti finanziari soggetti alla normativa, tuttavia il principio di proporzionalità resta applicabile. L'impatto di DORA è comunque ampio, come evidenziato dall'indagine IDC, secondo cui il 38% degli intervistati indica i test di resilienza operativa digitale come la sfida maggiore, mentre il 33% segnala la gestione del rischio legato a terze parti ICT come un ostacolo significativo.

La gestione del rischio coinvolge nuovi attori oltre alle funzioni di controllo delle istituzioni finanziarie

DORA impone una gestione più rigorosa della governance dei fornitori terzi, ampliando il coinvolgimento interno nella gestione del rischio. Non solo l'IT, ma anche l'ufficio acquisti assume un ruolo chiave, come indicato nel regolamento e nei relativi standard tecnici.
Le istituzioni finanziarie devono modernizzare i processi di procurement per garantire una valutazione continua dei fornitori in termini di performance, conformità normativa e resilienza. DORA richiede anche l'integrazione di clausole specifiche nei contratti esistenti e futuri, il monitoraggio tramite un registro dei fornitori ICT e, se necessario, il coinvolgimento dei fornitori critici in test di penetrazione per individuare vulnerabilità.
Secondo un'indagine IDC di ottobre 2024, solo il 50% delle istituzioni finanziarie si sarebbe detto pronto a gennaio 2025 con la mappa delle funzioni critiche e dei relativi fornitori ICT. È quindi plausibile che l'ufficio acquisti diventi parte attiva del Sistema di Controlli Interni di Conformità, affiancando l'ICT Governance nel supporto alle funzioni di compliance e risk management.

Un'opportunità per il sistema finanziario

DORA, pur introducendo complessità, può catalizzare un cambiamento positivo. Rafforzare la resilienza digitale migliora sicurezza operativa e fiducia di investitori e clienti. Per i fornitori ICT, la conformità diventa un vantaggio competitivo, aprendo nuove opportunità di business.
Questo regolamento segna l'inizio di un percorso verso un sistema finanziario più resiliente e interconnesso, dove istituzioni e partner tecnologici che sfrutteranno questa opportunità guideranno un nuovo paradigma di innovazione e sicurezza.

MARIA ADELE DI COMITE
Research Director, IDC Financial Insights Corporate and Retail Banking, EMEA

> È URGENTE COLMARE LE LACUNE REGOLAMENTARI E COSTRUIRE UNA STRATEGIA DI RESILIENZA PER GARANTIRE STABILITÀ IN UN'ECONOMIA SEMPRE PIÙ COMPLESSA E DIGITALE.

Scansiona il QrCode per accedere all'abstract del report "IDC PlanScape: Last-Call DORA Compliance Checklist to Achieve Digital Operational Resilience"

Reportec

È ANCHE

bizzit.it

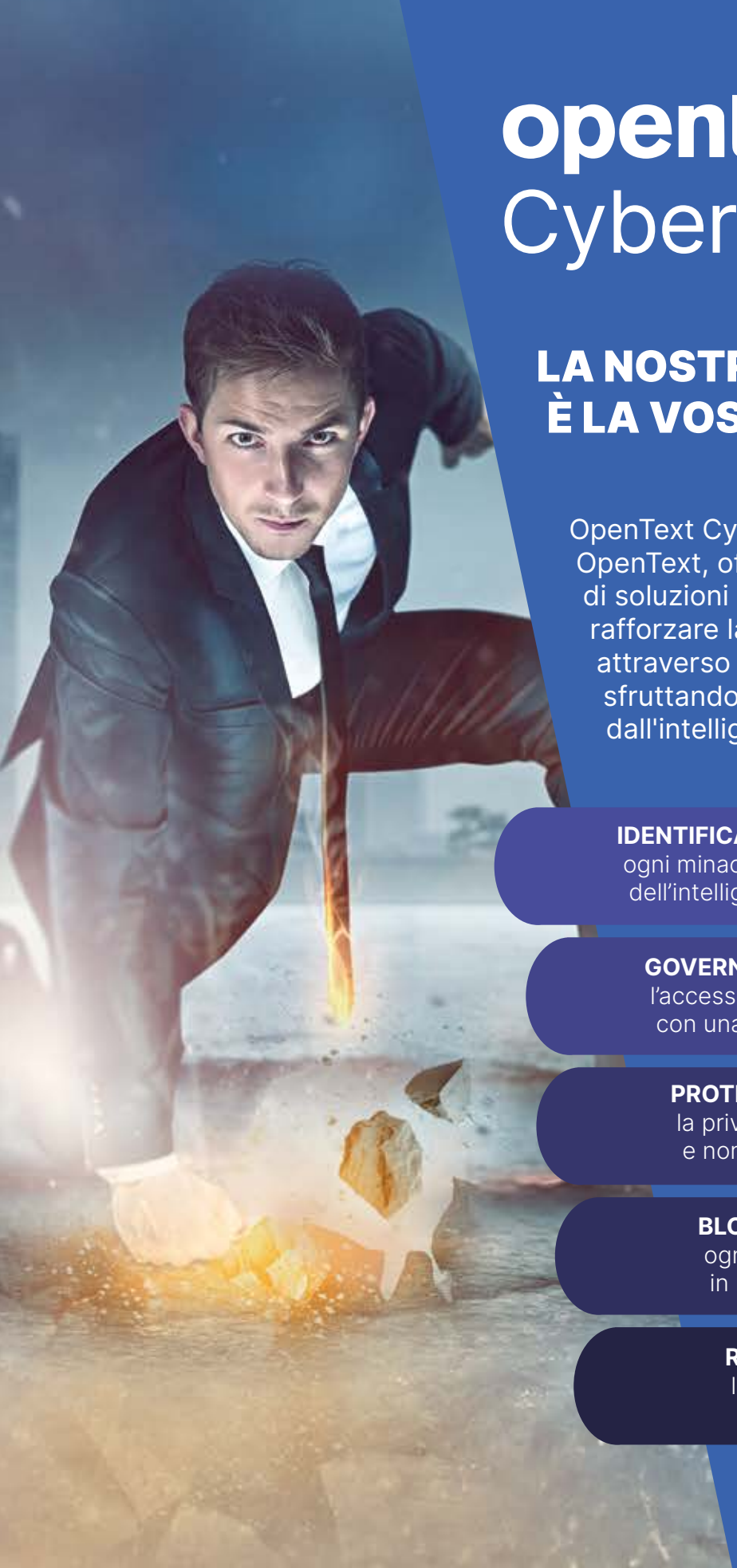
bizzIT.it è la rivista digitale che ti aggiorna con notizie, analisi, report, approfondimenti, interviste e case study dedicati all'ICT e alla tecnologia

bizzIT.it

INNOVAZIONI, TECNOLOGIE E NUOVE PROSPETTIVE

Iscriviti alle nostre newsletter

Redazione: REPORTEC srl | Via Gorizia 35/37
20099 Sesto San Giovanni (MI)
redazione@reportec.it | www.reportec.it



opentext™
Cybersecurity

LA NOSTRA FORZA È LA VOSTRA SICUREZZA

OpenText Cybersecurity, divisione di OpenText, offre il più ampio portafoglio di soluzioni modulari sul mercato per rafforzare la resilienza del tuo business attraverso il cloud e ambienti ibridi, sfruttando l'automazione guidata dall'intelligenza artificiale

IDENTIFICARE
ogni minaccia con la potenza dell'intelligenza artificiale

GOVERNARE
l'accesso e l'identità con una gestione Zero Trust

PROTEGGERE
la privacy e i dati strutturati e non strutturati

BLOCCARE
ogni tipo di minaccia e rispondi in modo rapido e proattivo

RAFFORZARE
la sicurezza delle applicazioni con analisi del codice e test

opentextcybersecurity.it