PARTNERS • NUMERO 66

PARTNERS

INFORMAZIONE E FORMAZIONE PER IL CANALE A VALORE

MARKET VIEW

COMPLIANCE NORMATIVA
LE LEGGI CHE
REGOLANO IL DIGITALE

FOCUS TECNOLOGIE

HYBRID CLOUD
E **MULTI-CLOUD,**
FACCIAMO CHIAREZZA

CYBER SECURITY
PREVISIONI, TREND
E REPORT 2025

INCHIESTA CANALE

OPEN SOURCE
IL MOTORE DELLA
TRASFORMAZIONE
DIGITALE

SENTINELONE
L'AI trasforma la cybersecurity
con Singularity

OPENTEXT CYBERSECURITY
Proteggere i dati nell'era dell'AI

ESET
Il futuro della sicurezza IT
tra AI e minacce emergenti

WITHSECURE
e **COMPUTER GROSS**
Le sfide nel 2025: minacce, normative
e nuove strategie di protezione

SOMMARIO

FEBBRAIO 2025 • N. 66

PARTNERS
Anno XIII - numero 66
Febbraio 2026

Direttore responsabile: Riccardo Florio
In redazione: Riccardo Florio, Paola Rosa

Hanno collaborato: Maurizio Ferrari, Fabrizio Pincelli, Leo Sorge

Redazione:
REPORTEC srl | Via Gorizia 35/37
20099 Sesto San Giovanni (MI);
Tel 339 3785157 | www.reportec.it |
redazione@reportec.it

Editore:
Reportec Srl, C.so Italia 50 | 20122 Milano

Diffusione: 35.000 copie digitali

Concessionaria pubblicitaria diretta
commerciale@reportec.it

Iscrizione al tribunale di Milano n° 515 del 13 ottobre 2011.
Immagini: Dreamstime.com

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

RICCARDO FLORIO
DIRETTORE RESPONSABILE

I rischi dell'AI non si risolvono solo con la tecnologia

L'intelligenza artificiale continua a essere "il tema" del dibattito informatico e grande attenzione si sta concentrando sugli aspetti dei rischi, come dimostrato dalle previsioni in materia di cybersecurity riportate in questo numero.

È opportuno, tuttavia, distinguere tra due categorie di rischi: da un lato, ci sono quelli associati all'uso dell'**AI per individuare e sfruttare vulnerabilità, produrre attacchi più sofisticati o malware** capaci di evitare le difese tradizionali e, dall'altro, i rischi derivanti dall'**impatto che l'AI generativa ha sul comportamento degli utenti**.

I rischi del primo tipo sono, in linea di principio, contrastabili mediante l'adozione di soluzioni tecnologiche, inclusa l'AI "buona". Grazie alla capacità di elaborare dati in tempo reale e di individuare anomalie si possono, per esempio, implementare sistemi di difesa proattivi, in grado di intercettare attacchi informatici prima che possano provocare danni rilevanti. Soluzioni basate su algoritmi di machine learning hanno già evidenziato una significativa riduzione dei tempi di risposta agli incidenti.

I rischi associati all'AI generativa invece, non possono essere contrastati meramente sul piano tecnologico e, per certi versi, interessano uno spettro d'azione più ampio.

Molti utenti operativi non solo non hanno comprensione dei rischi dei perimetri di utilizzo dell'AI, ma non ne sono neppure interessati. Come spesso capita nei contesti lavorativi odierni, sempre più veloci e con staff sottodimensionato, **l'esigenza o la pressione di chiude-**

RICCARDO FLORIO
DIRETTORE RESPONSABILE

re un lavoro supera le preoccupazioni sul livello qualitativo prodotto. Così il vantaggio di poter affidare all'AI una buona parte del proprio lavoro ne favorisce un uso piuttosto disinvolto e convince l'utilizzatore che, alla fine, il risultato prodotto è soddisfacente.

L'impiego inappropriato di questi strumenti può causare, per esempio, l'inserimento non consapevole di dati critici o sensibili nei motori di intelligenza artificiale che espone le organizzazioni a vulnerabilità che sfuggono ai tradizionali sistemi di difesa. Inoltre, la difficoltà degli utenti nel distinguere tra differenti modelli e motori di AI comporta il rischio di generare informazioni errate o di compromettere la riservatezza dei dati.

In aggiunta ai rischi di compromissione di informazioni importanti emergono, quindi, anche **potenziali danni di immagine, errori contabili, compromissioni inconsapevoli del diritto d'autore o la creazione di documenti e dati errati** che possono alterare il buon esisto di processi operativi, campagne marketing o decisioni aziendali.

A livello tecnologico i rischi dell'AI si fronteggiano attraverso un continuo **aggiornamento di sistemi e software** di monitoraggio e risposta alle minacce. Per affrontare i rischi del secondo tipo servono invece investimenti in **programmi di formazione mirati**, finalizzati a sensibilizzare e preparare gli utenti sull'utilizzo responsabile delle tecnologie AI e la comprensione di limiti e potenzialità associati.

In parallelo, appare sensato e auspicabile che le aziende introducano **regolamentazioni interne per monitorare e controllare l'utilizzo indiscriminato dell'AI generativa**. Si tratta di un compito non facile poiché un approccio eccessivamente restrittivo rischia di compromettere il potenziale innovativo abilitato dall'AI.

Una strada certamente efficace sarebbe quella di non limitare l'uso dello strumento ma, invece, di esercitare il controllo sui dati accessibili da parte dei modelli di GenAI utilizzando unicamente repository interni e/o controllati. Si tratta di una strada possibile, su cui si stanno muovendo alcune aziende, ma che va percorsa con partner qualificati (difficili da trovare) e che richiede, comunque, investimenti e competenze non alla portata di tutti.

Image: Freepik

Cybersecurity 2025: i trend, le previsioni, i report

Il panorama della sicurezza informatica si prepara a trasformazioni radicali in vista del 2025. La crescita degli attacchi basati sull'intelligenza artificiale, il ruolo della cyber-resilienza, l'evoluzione delle minacce, l'espansione degli ambienti OT e cloud, le criticità nel software e il rafforzamento delle normative delineano un futuro complesso e dinamico. Le previsioni dei vendor.

di **Riccardo Florio**

In un'epoca in cui la rivoluzione digitale accelera la trasformazione di ogni settore, le minacce informatiche si fanno sempre più sofisticate, interconnesse e in costante evoluzione. **Le previsioni per il 2025, elaborate da molteplici realtà del settore**, offrono un quadro articolato e multi-fonte delle sfide future: dalla crescente pericolosità degli attacchi AI-driven alla sicurezza degli ambienti industriali, dalla protezione nel cloud all'adozione di normative integrate.

Intelligenza artificiale: un'arma a doppio taglio

Tutti concordano sul fatto che **il ruolo dell'intelligenza artificiale (AI) nella cybersecurity diventerà centrale nel 2025**, sia per potenziare le difese sia come strumento nelle mani de-

gli aggressori. Infatti, l'uso dell'AI in ambito cybersecurity da un lato, offre strumenti avanzati di difesa, dall'altro consente ai cybercriminali di lanciare attacchi sempre più sofisticati: per esempio per produrre attacchi Deepfake e di phishing.

Secondo **SentinelOne** la maggior parte delle aziende che stanno rapidamente integrando l'AI nei loro prodotti si rivolgerà a piattaforme di AI ospitate in cloud e questa nuova superficie di attacco aprirà opportunità per gli hacker. Un possibile modello che si diffonderà nel 2025 (già usato nel 2024) prevedrà che gli aggressori dirottino i servizi di AI in hosting nel cloud per utilizzare l'infrastruttura delle vittime per **creare un'applicazione LLM che fornisca interazioni non conformi** alle consuete protezioni integrate nel servizio.

WatchGuard sottolinea come nel 2025 i sistemi di AI multimodale acquisiranno progressivamente la capacità di integrare testo, immagini, voce e codici complessi e, di conseguenza, **l'AI verrà utilizzata dai cybercriminali per ottimizzare e automatizzare l'intera pipeline di un attacco informatico**. Questo includerà il profilare i bersagli sui social media, creare e inviare contenuti di phishing realistici, inclusi attacchi vocali (vishing), scoprire talvolta exploit di tipo zero-day, generare malware in grado di eludere i sistemi di rilevamento degli endpoint, implementare l'infrastruttura necessaria a supportarlo, automatizzare i movimenti laterali all'interno delle reti compromesse ed esfiltrare i dati rubati (QUI le previsioni complete).

Vectra AI prevede che nel 2025 assisteremo anche a uno spostamento dai copilot della sicurezza verso sistemi di intelligenza artificiale più autonomi progettati per funzionare in modo indipendente. In particolare, il settore della cybersecurity rivolgerà la sua attenzione ai modelli di **Agent AI** (modelli autonomi in grado di suddividere compiti complessi in sotto-attività e operare in modo indipendente) come mezzo principale per creare sistemi di intelligenza artificiale automatizzati per analizzare interi cicli di attacco.

Anche **Kaspersky** sottolinea il legame tra AI e attacchi e l'evoluzione verso sistemi Agent AI. Secon-

LEGGI QUI
LE PREVISIONI COMPLETE

do un recente report pubblicato dal vendor il 77% dei professionisti italiani intervistati ha osservato **un aumento degli attacchi informatici e il 43% ritiene che l'incremento sia direttamente legato all'uso dell'AI**. Le aziende dovranno, secondo il vendor, investire necessariamente in tecnologie difensive basate sull'AI e in una formazione continua del personale. Oltre a dover fronteggiare attacchi sempre più mirati, le aziende dovranno affrontare anche un fenomeno crescente: la **manipolazione delle informazioni tramite AI**.

La disinformazione sarà un problema di sicurezza informatica non solo per i governi, ma anche per le aziende, con il rischio di campagne mirate per destabilizzare il mercato o influenzare il valore azionario delle società. Gli analisti prevedono che nel 2025, la maggioranza delle fake news sarà generata proprio dall'intelligenza artificiale.

SCARICA IL REPORT CYBER DEFENSE & AI: SONO PRONTE LE AZIENDE A PROTEGGERSI?

Trend Micro mette in guardia chi sottovaluta questi rischi e sostiene che, nel 2025, l'AI sarà utilizzata in maniera sempre più sofisticata per la manipolazione di dati personali e per **realizzare campagne di phishing e che i Deepfake non saranno solo un fenomeno mediatico**, ma uno strumento cardine per le frodi digitali, utilizzate per ingannare utenti e sistemi di autenticazione.

CYBERSECURITY: NEL 2025 L'AI SARÀ LA PROTAGONISTA

Clicca qui per approfondire

A livello di difesa, i fornitori di cybersecurity stanno lavorando per implementare soluzioni avanzate di **AI explainability** ovvero in grado di rendere trasparenti e comprensibili le decisioni prese dagli algoritmi di sicurezza. Questa funzione permetterà ai team SOC di capire con maggiore precisione come vengono identificate le minacce e quali contromisure adottare per migliorare i sistemi di protezione.

Un altro fenomeno emergente riguarda gli **attacchi automatizzati ai modelli di Machine**

learning. I criminali informatici stanno iniziando a inserire dati corrotti nei modelli di intelligenza artificiale utilizzati per la sicurezza, alterandone il comportamento e riducendo la loro affidabilità. Secondo diversi analisti entro il 2025 vedremo un incremento nei **tentativi di compromissione mirata ai dataset di training delle infrastrutture di AI**.

Le minacce aumentano ed evolvono

Il ransomware continua a rappresentare una delle minacce più insidiose e in evoluzione. Le previsioni per il 2025 evidenziano non solo un aumento di questi attacchi, ma anche l'evoluzione del modello **ransomware-as-a-service (RaaS)** che rende le campagne di estorsione accessibili anche a gruppi con competenze tecniche limitate.

COS'È IL RANSOMWARE AS A SERVICE (RAAS)

Clicca qui per approfondire

Secondo **Eset** gli **infostealer** saranno anche per il 2025 **tra le minacce maggiormente diffuse a livello internazionale**, affiancandosi a una nuova ondata di truffe sui social media che utilizzano video Deepfake e post aziendali falsificati per attirare le vittime in piani di investimento fraudolenti.

SCARICA IL REPORT THREAT REPORT H2 2024

WithSecure conferma per il 2025 un trend preoccupante (già sottolineato nel report del 2024 report *Mass exploitation: The vulnerable edge of enterprise security*) relativo alla **"mass exploitation" dei servizi Edge e dell'infrastruttura come vettore d'infezione**. Secondo il vendor nel 2025 questo trend aumenterà ulteriormente rendendo la mass exploitation il vettore primario per gli attacchi ransomware e lo spionaggio di stato superando le Botnet. I servizi Edge rappresentano un obiettivo privilegiato per essere attaccati da remoto proprio per la loro natura che li rende esposti a Internet e progettati per fornire servizi critici a utenti remoti.

SCARICA IL REPORT MASS EXPLOITATION: THE VULNERABLE EDGE OF ENTERPRISE SECURITY

Kyndryl sottolinea anche che **le aziende del settore bancario, dei pagamenti e dei mercati dei capitali** nel 2025 sfrutteranno l'intelligenza artificiale a supporto della cybersecurity e della conformità, adottandola all'interno di soluzioni per i controlli normativi, la rilevazione delle frodi e la protezione dei dati dei consumatori. Inoltre, ci si aspetta una crescita nell'uso dell'IA generativa nel campo dell'antiriciclaggio per identificare in modo più accurato attività sospette.

LEGGI QUI
LE PREVISIONI COMPLETE

Akamai Technologies nelle sue **previsioni per il 2025** sottolinea anche i potenziali rischi legati all'intensificarsi di attacchi alle **Application programming Interfaces (API)**, ormai fondamentali per l'integrazione e l'automazione dei processi aziendali, ma spesso meno protette rispetto ad altre componenti dell'infrastruttura IT, che espongono le aziende a potenziali ripercussioni significative in termini di esposizione dei dati e interruzione delle operazioni.
Altre tecnologie poco monitorate, nel mirino attuale dei criminali informatici, sono i dispositivi di rete periferici (come firewall, router e switch) e gli smartphone.
Inoltre, le aziende dovranno affrontare un **incremento degli attacchi fileless**, ossia attacchi che non utilizzano malware tradizionale ma sfruttano strumenti e script nativi del sistema operativo. Questo tipo di minaccia sarà sempre più diffuso nei tentativi di compromissione della supply chain del software, rendendo inefficaci molte tecniche di rilevamento basate su firma digitale.
Da segnalare anche **la sicurezza dei droni e dei sistemi satellitari tra le nuove frontiere di rischio** meritevoli dell'adozione di tecnologie avanzate quali, per esempio, crittografia robusta e sistemi di rilevamento intrusioni su misura (ma servirà anche entro breve una cooperazione internazionale per definire standard condivisi).

THE YEAR IN REVIEW 2024: TODAY'S INSIGHTS, TOMORROW'S OUTLOOK

Clicca qui
per approfondire

Cyber-resilienza e XDR

Le aziende stanno sempre più puntando sulla cyber-resilienza, adottando strategie per prevenire e mitigare le minacce. **Le piattaforme XDR continueranno anche nel 2025 a essere ampiamente apprezzate dalle aziende** con l'obiettivo di ridurre il tempo di identificazione delle minacce e predisporre modelli automatizzati di risposta. Un'evoluzione in corso vede sempre più questo tipo di soluzioni offerte anche in modalità di Managed services.

Secondo **Barracuda Networks**, nel 2025 le minacce informatiche diventeranno ancora più mirate e adattive e i criminali informatici sfrutteranno l'AI e gli attacchi basati sul machine learning per colpire i vettori in modo sempre più personalizzato e veloce. Di conseguenza **l'XDR si evolverà oltre il monitoraggio reattivo per diventare la spina dorsale delle operazioni di sicurezza predittive** e automatizzate. Le piattaforme XDR si integreranno con ecosistemi più ampi come SOAR e la **Threat intelligence guidata dall'AI**, consentendo una valutazione dinamica del rischio e risposte prioritarie tra cloud, endpoint, rete e altro.

7 SECURITY PREDICTIONS FOR 2025 FROM BARRACUDA EXECUTIVES

Clicca qui per approfondire

Nel contempo, l'integrazione di tecniche basate sull'AI metterà a disposizione anche degli aggressori nuovi strumenti per automatizzare l'esfiltrazione dei dati, bypassare sistemi di autenticazione multifattoriale e cercare di neutralizzare le contromisure difensive offerte dalle soluzioni EDR e XDR. Questo scenario porterà le aziende a ripensare le proprie strategie di cyber resilienza difensive, guardando verso **misure sempre più proattive quali la segmentazione della rete, piani di recupero dati rapidi** e una formazione costante per riconoscere i vettori di attacco emergenti.

Secondo **Robert Haist**, CISO di **TeamViewer**, il 2025 sancirà anche **la fine dell'era BYOD** (Bring your own device), che non rappresenta più una scelta strategica per le aziende attente alla sicurezza e che intendono rafforzare le procedure e migliorare le risposte alle minacce in continua evoluzione.

Axis Communications fa notare anche l'impatto che avrà nel 2025 l'evoluzione nella qualità delle immagini unita ai progressi nel campo dell'analisi e dell'IA, che renderà più accurato il riconoscimento degli oggetti e porterà alla creazione di dati e metadati sempre più dettagliati oltre che a un ampliamento dell'area di copertura ottenibile tramite una singola telecamera di sorveglianza.

La sicurezza delle infrastrutture critiche e degli ambienti OT

Nel 2025 i rischi per le infrastrutture critiche si configureranno in maniera ancora più preoccupante, a causa dell'integrazione sempre più profonda dei sistemi digitali in settori strategici come energia, trasporti, sanità e telecomunicazioni. Le previsioni per il 2025 indicano che settori quali smart city, reti elettriche, sanità e perfino risorse spaziali diventeranno obiettivi privilegiati per attacchi sempre più sofisticati.

Un dato confermato anche dall'ultimo report **Enisa Threat Landscape 2024 (scaricabile QUI)**, che evidenzia come le vulnerabilità nei sistemi industriali e nelle reti di comunicazione siano aumentate del 30% negli ultimi anni, segnale che la convergenza tra cyberattacchi e tensioni geopolitiche sta alimentando una nuova era di cyberwar.

La crescente integrazione dei **sistemi di controllo industriale (OT)** nelle infrastrutture critiche e la loro contestuale evoluzione verso modelli che si aprono per la prima volta all'esterno, inserisce anche questi sistemi nelle superfici d'attacco. Le soluzioni di sicurezza IT tradizionali spesso non sono adatte agli ambienti OT a causa di requisiti e vincoli unici dei sistemi di controllo industriali e **le aziende del settore stanno integrando soluzioni specifiche per proteggere gli ambienti OT,** cercando di colmare il divario tra le tecnologie di sicurezza IT tradizionali e le esigenze peculiari degli ambienti industriali.

Di conseguenza, **Nozomi Networks** sottolinea che nel 2025 con ogni probabilità vedremo vendor che vantano una presenza consolidata nel mondo della cybersecurity tradizionale aprirsi verso il mondo OT attraverso fusioni e acquisizioni, partnership strategiche e lo sviluppo di prodotti specializzati.

Claroty nel **report State of CPS Security 2025**: OT exposures evidenzia come il 12% delle organizzazioni intervistate disponesse di asset OT che risultavano comunicare con domini malevoli. Questo vendor sottolinea anche come il tema delle cyber resilienza nel 2025 entrerà in modo prepotente anche nell'ambito sanitario con una cybersecurity in evoluzione da una posizione prevalentemente reattiva a una proattiva, guidata dai principi definiti dall'ENISA e ispirati al framework NIST, per anticipare, resistere, adattarsi e riprendersi dalle minacce: un cambiamento che si rende oggi quanto mai essenziale per mitigare l'impatto di attacchi come i ransomware, che rimangono una minaccia significativa per ospedali e fornitori di servizi sanitari.

SCARICA IL REPORT STATE OF CPS SECURITY: OT EXPOSURES 2025

Cloud e gestione della postura di sicurezza

Il passaggio massiccio verso il cloud ha rivoluzionato la gestione dei dati e delle infrastrutture aziendali. **Nel 2025 la protezione degli ambienti cloud diventerà una priorità strategica**, poiché l'aumento dei dati e l'evoluzione degli attacchi richiederanno soluzioni sempre più sofisticate.
Nel 2024, secondo il **CrowdStrike Global Threat Report 2024**, le intrusioni nel cloud sono aumentate del 75% rispetto all'anno precedente, evidenziando come le vulnerabilità in ambienti ibridi e multi-cloud rappresentino una sfida crescente per le aziende.
Questo trend continuerà anche nel 2025 favorendo la diffusione di **soluzioni per la gestione della postura di sicurezza dei dati (Data Security Posture Management, in sigla DSPM)** per ottenere una migliore visibilità sullo stato di protezione dei dati distribuiti e un monitoraggio in tempo reale tramite soluzioni AI-driven.

Il nuovo ruolo del CISO

Parallelamente alle minacce, anche il ruolo del Chief Information Security Officer (CISO) è in trasformazione: le crescenti richieste normative e il peso delle responsabilità stanno rendendo questa posizione sempre meno attrattiva.

Secondo **WatchGuard** nel 2025 e negli anni a venire questa pressione crescente potrebbe aumentare il turnover, riducendo l'attrattiva per i candidati qualificati disposti a ricoprire tale ruolo causando difficoltà per le aziende nel reperire profili di questo tipo. Nel 2025 le aziende, soprattutto della fascia medio-piccola, intensificheranno il ricorso a soluzioni esternalizzate, come i Managed security services, per ovviare alla carenza di competenze e garantire una protezione continua e una gestione efficace degli incidenti.

Normative e compliance, da NIS2 a DORA

L'evoluzione normativa rappresenta un altro aspetto cruciale per il 2025. In Europa, l'entrata in vigore del **Digital Operational Resilience Act (DORA) e l'arrivo della seconda versione della Direttiva NIS** impongono nuovi standard di sicurezza, costringendo le aziende a ripensare completamente le proprie strategie di protezione.

Queste normative mirano a rafforzare la resilienza operativa di settori strategici, come quello finanziario, le infrastrutture critiche e i servizi pubblici. I responsabili IT e i CISO dovranno adeguarsi a processi rigorosi, dalla gestione del rischio alla segnalazione degli incidenti, per ottenere vantaggi competitivi e rafforzare la fiducia di clienti e stakeholder.

Secondo **Rubrik** **nel corso del 2025 l'importanza di DORA andrà oltre l'ambito iniziale** e questo regolamento diventerà uno **strumento di resilienza operativa generale**, grazie alla sua serie di processi per la gestione del rischio, la segnalazione degli incidenti, la gestione del rischio di terzi e la gestione della continuità operativa. Una più estesa adozione di DORA ridefinirà, quindi, il modo in cui tutte le aziende affrontano la resilienza e la continuità operativa.

Un cybercrimine sempre più organizzato

Le previsioni per il 2025 dipingono un panorama in cui il cybercrime si organizza in maniera sempre più strutturata e industriale. I criminali informatici operano come vere aziende, con ruoli definiti e una presenza consolidata

nel dark web, sfruttando strumenti automatizzati basati sull'AI per lanciare attacchi sofisticati.
La crescente collaborazione tra hacktivisti e gruppi APT, unita all'uso di tecniche di Deepfake e ingegneria sociale, creerà nuove sfide per le difese tradizionali. Anche gli attacchi alla supply chain, in particolare nei progetti open-source, intensificheranno la necessità di un monitoraggio costante e di valutazioni periodiche delle vulnerabilità, spingendo le aziende ad adottare approcci zero trust.

Sicurezza nell'intero ciclo di sviluppo del software

Con questo aumento delle minacce informatiche, la sicurezza nel 2025 e negli anni a seguire cesserà di essere un elemento secondario del processo di sviluppo. Secondo **OpenText Cybersecurity** nel 2025 assisteremo a un **ulteriore diffusione dell'approccio DevSecOps**, che enfatizza l'integrazione dei controlli di sicurezza in tutto il processo di sviluppo, dalla scansione del codice al monitoraggio del runtime, sottolineando l'importanza d'implementare la modellazione delle minacce fin dalla fase di progettazione. **Nel 2025, secondo questo vendor, l'intelligenza artificiale e il machine learning rivoluzioneranno i flussi di lavoro DevOps**, passando da tecnologie sperimentali a pilastri fondamentali capaci di automatizzare compiti ripetitivi, prevedere potenziali criticità e ottimizzare i processi.
Altro tema centrale per garantire la sicurezza dello sviluppo software sarà **prevenire le vulnerabilità del codice open source,** con gli attaccanti che, nel 2025, intensificheranno i tentativi di prendere di mira librerie open-source e dipendenze poco conosciute (ma ampiamente utilizzate) per evitare il rilevamento ed eseguire attacchi malevoli.
A tale riguardo un report **Xygeni** sottolinea come, **nel 2025, i principi Zero Trust si espanderanno alla supply chain del software,** enfatizzando la verifica continua di ogni dipendenza, integrazione e interazione con l'utente in modo da garantire che solo i componenti affidabili e sicuri entrino nelle pipeline di sviluppo.

SCARICA IL REPORT THE STATE OF SOFTWARE SUPPLY CHAIN SECURITY IN 2025

Marco Rottigni,
technical director

SentinelOne l'AI trasforma la cybersecurity con Singularity

di **Leo Sorge**

Paolo Cecchi,
regional sales director
Mediterranean Region

L'AI integrata nella piattaforma Singularity garantisce una protezione avanzata contro le minacce sofisticate. Accelera il rilevamento, migliora la gestione degli incidenti e facilita la conformità normativa, potenziando la sicurezza delle infrastrutture aziendali.

L'intelligenza artificiale non è solo uno strumento, ma il cuore pulsante di un sistema in grado di proteggere le aziende da minacce sempre più complesse e sofisticate. **SentinelOne** propone una piattaforma avanzata e flessibile, che copre diverse superfici di attacco e si integra perfettamente con l'ecosistema IT delle organizzazioni.

Ne abbiamo parlato con due dirigenti di SentinelOne, **Paolo Cecchi, regional sales director Mediterranean Region**, e **Marco Rottigni, technical director**.

La vostra vision è ambiziosa: creare la piattaforma di cybersecurity più avanzata sul mercato, potenziata dall'intelligenza artificiale Purple AI. Cosa differenzia la vostra piattaforma da altri competitor?

Cecchi. I due aspetti fondamentali sono l'AI, su cui SentinelOne si ritiene leader grazie alla lunga e approfondita esperienza acquisita, e la più ampia copertura. La nostra piattaforma, infatti, protegge diverse superfici di attacco, integrando in modo nativo la telemetria e i dati provenienti da

endpoint, dispositivi mobili e sistemi legacy. Questa integrazione consente di gestire in modo efficace anche i complessi ambienti dell'OT, spesso trascurati dalle soluzioni tradizionali.

Rottigni. SentinelOne ha integrato l'intelligenza artificiale in tutta la piattaforma Singularity. Ad esempio, l'AI è in grado di interpretare i log e fornire agli analisti un contesto chiaro e logico degli incidenti, accelerando il processo di triage. Inoltre, gli analisti possono chiedere all'AI di generare script o reagire in tempo reale agli incidenti, migliorando ulteriormente la rapidità e l'efficacia delle operazioni. Bisogna evitare di inserire l'AI solo in una applicazione e non ovunque ecco perché SentinelOne si impegna a implementare soluzioni di difesa avanzate e pervasivamente integrate nella piattaforma, in modo che gli attaccanti non siano mai un passo avanti.

E cosa vi differenzia nella protezione del cloud?

Cecchi. SentinelOne offre una protezione avanzata del cloud attraverso CWP, Cloud Workload Protection, e CNAPP, una soluzione agentless di Cloud-Native Application Protection ed è questo approccio che permette di individuare configurazioni errate e vulnerabilità negli ambienti cloud con la mentalità di un attaccante, prioritizzando le minacce in base al reale rischio per l'organizzazione.

ASTON MARTIN ARAMCO DI FORMULA UNO SPINGE SULLA SICUREZZA CON SENTINELONE

Il Team ha scelto com SentinelOne come partner ufficiale per la cybersecurity, avvalendosi di soluzioni basate sull'AI per operare in modo sicuro dentro e fuori dal circuito.

Clicca qui
per approfondire
questo caso di successo

Come affrontate il tema delle vulnerabilità?

Cecchi. Uno dei problemi più diffusi nei sistemi di vulnerability management è la difficoltà di assegnare la corretta priorità alle minacce. Grazie all'approccio offensive, SentinelOne è in grado di simulare il percorso di un at-

taccante, identificando le vulnerabilità più critiche e offrendo ai clienti una strategia mirata per mitigare i rischi.

Che ruolo giocate nell'attuale contesto normativo delle aziende?

Cecchi. SentinelOne supporta le aziende nel rispondere ai requisiti di normative come la NIS2 e il nuovo regolamento Dora, seppur non coprendo ogni aspetto regolamentare. La vera difficoltà per le aziende sta nella traduzione dei requisiti normativi in operatività concreta e noi contribuiamo a colmare questo gap, fornendo strumenti che migliorano la conformità rispetto ai requisiti normativi in ambito cybersecurity.

Quali sono le direttrici tecnologiche sulle quali vi muovete?

Rottigni. Oggi le quantità di dati sono enormi, le fonti sono estremamente disomogenee e il tempo necessario per comprendere cosa un dato deve dirci è ridotto, quindi dare un vantaggio di tempo amplifica le capacità degli analisti. Noi stiamo lavorando su due fronti: l'evoluzione della nostra soluzione Purple AI, in modo che dia dei semilavorati sempre migliori, e un nuovo concetto di automazione, che chiamiamo Hyperautomation basata sul principio di costruzione flussi con approccio no-code.

Nella pratica, come avete introdotto l'AI?

Rottigni. SentinelOne ha fatto dell'intelligenza artificiale il cuore delle proprie attività di ricerca e innovazione già da una decina di anni. L'adozione di un sistema di rilevamento basato sull'intelligenza artificiale ha offerto enormi vantaggi: il sistema identifica minacce note ma anche sconosciute, semplificando la gestione delle infrastrutture aziendali e riducendo la necessità di aggiornamenti costanti su migliaia di dispositivi.

Come viene usata oggi l'AI in cybersecurity?

Rottigni. L'AI potenzia le competenze e l'efficacia degli analisti, accelerando il lavoro e migliorando le capacità. Nella mia esperienza, non ho ancora incontrato un cliente che avesse le security operation sovrastaffate, quindi non vedo il problema di abbattere i costi riducendo le risorse. Vedo invece il problema di accelerare i tempi di apprendimento per analisti giovani, e un'AI che non richiede un linguaggio di query ma parla la nostra lingua aiuta l'apprendimento in maniera tangibile e misurabile.

CYBERSECURITY

Proteggere i dati nell'era dell'AI

di **Riccardo Florio**

In un contesto sempre più digitale e interconnesso, proteggere i dati aziendali è una necessità imprescindibile. OpenText Cybersecurity offre soluzioni avanzate che combinano crittografia, automazione intelligente e gestione del rischio per garantire la massima sicurezza e conformità.

Pierpaolo Alì,
director Southern Europe di OpenText Cybersecurity

In un panorama tecnologico sempre più frammentato e dinamico, la protezione dei dati diventa un elemento strategico per la competitività delle aziende in cui l'esigenza di tutelare i propri asset si fonde con quella di conformarsi a normative sempre più stringenti.
OpenText Cybersecurity propone un approccio integrato e pragmatico alla sicurezza, puntando su una gestione intelligente del rischio, una protezione end-to-end e una visione unificata sulle minacce. Non si tratta di aggiungere un ulteriore livello di difesa, ma di **ripensare la cybersecurity come un processo continuo di prevenzione, rilevamento e risposta.**

Oltre il perimetro: protezione distribuita e sicurezza data centrica

Il modello di sicurezza data-centrico di OpenText Cybersecurity **sposta il**

focus dalla difesa delle infrastrutture alla protezione del dato indipendentemente da dove si trovi. Questo approccio non è solo una scelta logica, ma una necessità imprescindibile nell'attuale scenario digitale, in cui il concetto di perimetro aziendale si è dissolto a favore di un ecosistema decentralizzato, fatto di dati in continuo movimento e accessi distribuiti su più piattaforme e dispositivi.

La famiglia di soluzioni di **OpenText Cybersecurity per la Data Privacy and Protection** include tecnologie di crittografia avanzata, tokenizzazione e gestione degli accessi condizionati, che limitano il rischio di esfiltrazione e compromissione. Attraverso la protezione trasparente dei dati sensibili e la possibilità di gestire policy granulari di accesso, le aziende possono controllare chi e come può accedere alle informazioni, senza subire un impatto negativo sulle prestazioni.

Queste soluzioni si distinguono per la capacità di garantire una protezione avanzata dei dati a livello di file e database senza comprometterne l'usabilità. **Grazie alla crittografia dinamica, le aziende possono applicare protezioni su dati in uso, in transito e a riposo**, mantenendo il pieno controllo su chi può visualizzare o modificare le informazioni.

Attraverso le sue tecnologie esclusive, infatti, OpenText Cybersecurity consente di mascherare i dati (persino agli operatori) **rendendoli inutili per gli aggressori ma mantenendone, al contempo, l'usabilità, l'utilità e l'integrità referenziale** per i processi, le applicazioni e i servizi relativi ai dati, sia che si tratti di produzione, di sistemi analitici o di sistemi di test o di sviluppo.

"Le nostre soluzioni di Data Privacy and Protection - spiega **Pierpaolo Alì, director Southern Europe di OpenText Cybersecurity** - *offrono un livello di sicurezza senza precedenti, permettendo alle aziende di proteggere i propri asset digitali in un contesto di minacce in continua evoluzione. La nostra capacità di combinare crittografia avanzata, automazione intelligente e gestione adattiva del rischio ci consente di offrire una protezione superiore rispetto a qualsiasi altra soluzione sul mercato".*

Rispetto ai competitor, **OpenText Cybersecurity offre anche il vantaggio di un'integrazione nativa con ambienti multi-cloud**, garantendo un livello di protezione uniforme e centralizzato su qualsiasi piattaforma. Inoltre, la combinazione con funzionalità di monitoraggio continuo e di risposta automatizzata agli incidenti riduce i tempi di reazione alle minacce, migliorando l'efficacia complessiva della sicurezza.

Le aziende che operano in settori altamente regolamentati, come finanza, sanità e pubblica ammi-

nistrazione, traggono particolare beneficio da queste soluzioni, poiché consentono loro di rispettare i requisiti normativi più stringenti senza sacrificare efficienza operativa. Grazie alla protezione integrata dei dati, le organizzazioni possono evitare sanzioni per il mancato rispetto delle normative sulla privacy e mitigare i rischi derivanti da attacchi informatici mirati.

AI per la protezione dei dati

"Un interrogativo che in questo momento molti si stanno ponendo è come debba cambiare la protezione dei dati nell'era dell'AI - osserva Alì -. *La risposta è che, in un contesto in cui l'AI mette a disposizione dei cybercriminali nuovi strumenti per sferrare attacchi più efficaci, è sempre l'AI lo strumento di elezione per contrastarli. Ma è una tecnologia complessa su cui non ci si può improvvisare e OpenText Cybersecurity conosce bene queste tecnologie perché già da molti anni le ha integrate all'interno delle proprie soluzioni software di sicurezza".*

L'intelligenza artificiale è un elemento chiave nella strategia di protezione dei dati di OpenText Cybersecurity. Grazie all'AI, è possibile, per esempio, identificare automaticamente dati sensibili, applicare protezioni appropriate e monitorare il loro utilizzo in tempo reale. Questo approccio riduce il rischio di perdita o furto di dati, garantendo che le informazioni critiche siano sempre protette, indipendentemente dal contesto operativo.

Le funzionalità avanzate di AI consentono anche di rilevare anomalie nei modelli di accesso ai dati, segnalando attività sospette prima che si trasformino in violazioni effettive. Inoltre, l'automazione basata sull'AI permette di applicare policy di sicurezza adattive, **aggiornando automaticamente le misure di protezione in base all'evoluzione delle normative e delle esigenze aziendali.** Questo garantisce non solo una maggiore sicurezza, ma anche una gestione più efficiente della compliance, riducendo la complessità operativa per i team IT e di cybersecurity. Infine, l'AI consente inoltre di effettuare **un'analisi predittiva dei dati**, migliorando la capacità delle aziende di prevenire potenziali violazioni prima che si verifichino.

OpenText Cybersecurity integra queste capacità con strumenti avanzati di rilevamento automatico delle minacce e con sistemi di protezione intelligente che adattano le difese aziendali in base al comportamento dell'utente e all'evoluzione delle minacce esterne. Grazie a un approccio basato su AI, OpenText Cybersecurity riesce, quindi, a fare in modo che la protezione dei dati si mantenga costantemente aggiornata e dinamica, anticipando le minacce e adattandosi ai nuovi scenari digitali in modo proattivo.

Il futuro della sicurezza IT tra AI e minacce emergenti

di **Samuele Zaniboni**
manager of sales engineering, ESET Italia

La sicurezza informatica sta attraversando una trasformazione profonda e sta diventando una priorità strategica globale che coinvolge ogni settore. Analizzando le tendenze per il 2025, emergono alcuni aspetti chiave che delineeranno il futuro della cybersecurity.

La criminalità informatica come industria organizzata

Il cybercrimine evolve verso modelli strutturati, con ruoli definiti e operazioni simili a quelle aziendali. Attraverso il dark web, i criminali mantengono un alto livello di anonimato, incrementando la sofisticazione delle minacce, come malware bancari, infostealer e Ransomware-as-a-Service. Secondo l'ultimo **Threat Report H2 2024 di ESET**, gli infostealer restano tra le minacce più diffuse a livello internazionale, affiancati da truffe sui social media che utilizzano video deepfake e contenuti falsificati per attirare le vittime in piani di investimento fraudolenti.
Inoltre, si prevede un **aumento degli attacchi ransomware, integrati con "EDR killers"** per aggirare le soluzioni EDR e XDR.

L'AI: opportunità e rischio

Con le possibili evoluzioni geopolitiche, nel 2025 si ipotizza una deregolamentazione dei social media e delle aziende tecnologiche. Questo potrebbe portare a un aumento dei **contenuti di bassa qualità** generati dall'AI, inclusi spam, truffe e campagne di phishing, già osservabili nel 2024. Nel 2025, aumenteranno anche i **pro-**

fili falsi di celebrità e figure pubbliche sui social media, supportati da video deepfake e altri contenuti generati con l'AI, rendendo ancora più cruciale l'uso di strumenti di verifica dell'autenticità come i badge "verificati".

La sicurezza come elemento fondante della tecnologia

L'evoluzione della tecnologia richiede l'integrazione della sicurezza informatica fin dalle prime fasi di progettazione delle soluzioni. Machine learning, open source e collaborazione tra aziende e istituzioni saranno elementi fondamentali per costruire sistemi più resilienti. La tecnologia dovrà affiancarsi ai servizi di security H24 che combinano la potenza dell'AI con l'expertise di professionisti che operano nel settore della cybersicurezza.

L'approccio di ESET

ESET si pone come partner strategico per le aziende, offrendo soluzioni che combinano protezione endpoint, crittografia avanzata e sicurezza delle applicazioni cloud. Grazie a strumenti dedicati come la piattaforma di Managed detection and response (MDR), ESET garantisce un monitoraggio costante delle infrastrutture e una risposta rapida alle minacce.

SCARICA QUI IL THREAT REPORT H2 2024 DI ESET

Il Security operations center (SOC) italiano garantisce un supporto tempestivo e personalizzato in lingua madre, aiutando le aziende a gestire incidenti complessi in modo efficace.

Il **supporto ai partner** rappresenta un altro pilastro della strategia di ESET: formazione, risorse marketing e assistenza tecnica sono progettate per potenziare le competenze e accrescere il valore dell'offerta di cybersecurity.

Il 2025 rappresenta un anno cruciale, caratterizzato da minacce sempre più sofisticate e da un utilizzo crescente dell'AI.

Le organizzazioni dovranno adattarsi rapidamente, puntando sulla collaborazione tra stakeholder, l'adozione di tecnologie innovative e la resilienza dei sistemi. Garantire la sicurezza H24 sarà imprescindibile per proteggere dati e infrastrutture.

Le aziende che sapranno innovare senza compromettere la sicurezza saranno meglio posizionate per prosperare in un contesto sempre più digitale e interconnesso.

PER CONOSCERE LE SOLUZIONI **ESET**

Le sfide della cybersecurity nel 2025: minacce, normative e nuove strategie di protezione

sopra **Carmen Palumbo,**
country sales manager di WithSecure per l'Italia;
sotto **Barbara Ramaciotti,**
bu manager security di Computer Gross

Quali saranno i rischi maggiori? Come proteggersi, anche per essere conformi alle normative? Che ruolo avranno vendor, distributori e partner? Lo abbiamo chiesto a Carmen Palumbo, country sales manager di WithSecure per l'Italia, e Barbara Ramaciotti, business unit manager security di Computer Gross

di **Fabrizio Pincelli**

Il mondo della sicurezza informatica si evolve rapidamente e le minacce diventano sempre più sofisticate. Abbiamo incontrato **Carmen Palumbo, country sales manager di WithSecure per l'Italia**, e **Barbara Ramaciotti, business unit manager security di Computer Gross**, per parlare delle sfide del 2025 e delle strategie per affrontarle.ù

Quali ritenete possano essere le principali minacce informatiche per il 2025?

Palumbo. Il ransomware continua a evolversi, con gruppi criminali sempre più sofisticati che colpiscono infrastrut-

ture critiche come sanità, energia e trasporti. Uno dei fattori che faciliterà la diffusione delle minacce è l'intelligenza artificiale, che offre nuovi strumenti per automatizzare attacchi come phishing, malware e violazioni dei sistemi.
Inoltre, la **supply chain è un punto sempre più critico**: i cybercriminali sfruttano le interconnessioni tra le aziende per infiltrarsi nei sistemi. Anche il **cloud** presenta rischi, poiché configurazioni errate possono esporre dati sensibili.

Ramaciotti. Nel 2024, vendor e distributori hanno compiuto un grande sforzo per sensibilizzare i partner sulle nuove normative, come la direttiva NIS2, e per aiutarli a prepararsi adeguatamente. Quest'anno, il supporto rimarrà cruciale e la collaborazione tra vendor, distributori e partner sarà fondamentale per colmare le lacune e affrontare le sfide strutturali delle PMI, che spesso non dispongono delle competenze interne per gestire i nuovi requisiti tecnologici e normativi.
Il distributore gioca un ruolo strategico non solo nel trasferire competenze attraverso attività di formazione, ma anche nell'offrire un supporto concreto nelle fasi operative e strategiche.

Qual è il livello di preparazione delle imprese nei confronti delle nuove normative in tema di sicurezza?

Palumbo. L'adeguamento alla direttiva NIS2 è molto variabile. Non c'è una correlazione diretta tra dimensioni aziendali e adeguamento, dipende dalla visione strategica del management. Alcune aziende hanno adottato un approccio proattivo, verificando la propria posizione e avviando il processo di conformità. Molte altre, invece, non hanno ancora colto l'importanza della normativa. I partner di canale giocano un ruolo cruciale nel sensibilizzare queste aziende e guidarle nella comprensione delle nuove regole. La NIS2 non dovrebbe, però, essere vista solo come un insieme di obblighi, ma come un'opportunità per migliorare la resilienza operativa. Un ulteriore elemento di complessità è la normativa DORA, che riguarda la resilienza operativa digitale per le istituzioni finanziarie.

Questa evoluzione porterà i partner a essere ancor più coinvolti? Evolverà il loro ruolo?

Palumbo. I partner stanno assumendo un ruolo più strategico, passando **da semplici rivendi-**

tori a consulenti a tutto tondo. L'utente finale cerca un supporto che vada oltre la fornitura di tecnologia, includendo anche implementazione e supporto continuo. La vendita di licenze non è più sostenibile da sola: i clienti cercano un **interlocutore unico** e affidabile, in grado di garantire un servizio completo.

Ramaciotti. Le esigenze degli utenti finali sono più complesse e richiedono **soluzioni integrate**. Molti partner non hanno le risorse per gestire autonomamente questi servizi, rendendo il ruolo del distributore sempre più centrale. Noi supportiamo i partner con formazione e consulenza, aiutandoli nelle fasi iniziali per renderli indipendenti. Se necessario, offriamo anche una gestione continuativa dei servizi.

Se un'azienda vi chiedesse: *"Per il 2025 vorrei migliorare la mia postura di sicurezza"*, cosa consiglierete?

Palumbo. Anzitutto di effettuare un'analisi approfondita della rete per identificare vulnerabilità e definire strategie di mitigazione. Questo include l'adozione di firewall avanzati, sistemi di monitoraggio delle intrusioni e protezione contro phishing. È fondamentale anche la formazione degli utenti per ridurre il rischio di attacchi.
Per garantirsi una protezione costante e dinamica si può poi scegliere un servizio di monitoraggio continuo della rete gestito da partner specializzati.

Ramaciotti. Il nostro approccio è di instaurare un rapporto diretto e dedicato con il partner. Analizziamo perciò il contesto e comprendiamo le sue esigenze specifiche e dei suoi clienti. A tal fine, abbiamo introdotto la figura del **Security Specialist**, che aiuta nel processo di onboarding e identifica le aree di miglioramento. Questo ci permette di proporre soluzioni personalizzate e di coinvolgere i vendor appropriati a implementare le strategie più adeguate.
La cybersecurity è diventata una priorità strategica e sempre più aziende stanno investendo in formazione e sviluppo di competenze. Il futuro della sicurezza informatica dipenderà dalla capacità di creare un **ecosistema collaborativo tra vendor, distributori e partner**.

PER APPROFONDIRE

WITHSECURE clicca qui
COMPUTER GROSS clicca qui

Image: Freepik

Hybrid cloud e multi-cloud, facciamo chiarezza

Spesso si tende a confondere le due piattaforme, che invece hanno caratteristiche ben definite, ciascuna con vantaggi e sfide differenziati. Analizziamole in dettaglio per evidenziare quando proporre l'una o l'altra a un'azienda o addirittura implementarle entrambe

di **Fabrizio Pincelli**

Flessibilità, scalabilità, sicurezza, resilienza e risparmi sui costi. Sono queste le principali caratteristiche del cloud, caratteristiche che, in un primo momento, hanno convinto molte aziende ad abbandonare in modo repentino l'on-premise per migrare dati e applicazioni sulla nuvola. L'esperienza ha però insegnato che il cloud può portare notevoli vantaggi, ma anche che va affrontato in modo un po' più cauto perché non è detto che sia la soluzione migliore per tutte le situazioni. Infatti, se la cloud strategy non è parte di una chiara tattica di workload placement finalizzata a raggiungere gli obiettivi aziendali i **costi possono superare i benefici**. Concetto questo che, nel tempo, ha portato all'adozione di ambienti distribuiti come il **multi-cloud** e l'**hybrid cloud**, i quali, grazie anche allo sviluppo tecnologico, permettono di coniugare al meglio le opportunità offerte dal cloud con le esigenze aziendali.
Vediamo allora perché oggi un'a-

STRUMENTI PER LA GESTIONE DEL MULTI-CLOUD

Le organizzazioni che utilizzano un cloud singolo dovrebbero attenersi ai **servizi di gestione nativi** del proprio provider cloud per i carichi di lavoro cloud e al proprio stack di gestione dell'infrastruttura on-premise nella misura in cui supporta la piattaforma cloud scelta. Se si estende il workload ad altri ambienti cloud o si riscontrano limitazioni significative con gli strumenti integrati, come la mancanza di visibilità o il provisioning e l'analisi manuale rispetto a quella automatizzata, si dovrebbero invece usare **strumenti specifici per la gestione multi-cloud**. Un tempo, i software di terze parti colmavano lacune nelle capacità di gestione dei provider cloud, ma gli hyperscaler hanno notevolmente migliorato le loro piattaforme di gestione native. Strumenti come **AWS Cost Explorer** e **Microsoft Cost Management and Billing** includono funzionalità di analisi, reporting e ottimizzazione che un tempo si trovavano solo nei prodotti aggiuntivi. Inoltre, i provider di servizi cloud ora offrono anche framework in grado di semplificare la gestione dei workload tra cloud diversi. Per esempio, **Azure Arc** consente di gestire carichi di lavoro ospitati al di fuori di Azure utilizzando strumenti nativi di Azure. **Google Cloud Anthos** offre funzionalità simili. Questi sono poco flessibili perché richiedono che i workload siano configurati o distribuiti in modi specifici; per esempio, Anthos in genere funziona solo con ambienti basati su kubernetes. Tuttavia, hanno il vantaggio di essere integrati nelle piattaforme cloud pubbliche.

zienda dovrebbe scegliere uno o l'altro ambiente (o anche entrambi) e come un partner tecnologico può giocare un ruolo strategico nell'aiutarla a superare le sfide che si possono presentare nell'ottimizzazione della gestione delle proprie risorse IT. Senza trascurare che l'adozione sempre più diffusa dell'intelligenza artificiale (AI) sta accelerando **il mercato del cloud in Italia**, che nel 2024 ha registrato una **crescita del 24%** rispetto all'anno precedente, raggiungendo un valore complessivo di 6,8 miliardi di euro. Secondo l'ultima ricerca dell'*Osservatorio Cloud Transformation* del Politecnico di Milano, questo incremento rappresenta il più alto degli ultimi sei anni, superando persino il +20% registrato nel 2020, in piena pandemia.

Multi-cloud, per avere sempre il meglio

Il multi-cloud e l'hybrid cloud rappresentano soluzioni strategiche con vantaggi distintivi e peculiari. Perciò avere chiare le differenze, le potenzialità e i limiti è fondamentale per adottare una strategia efficace e allineata agli obiettivi aziendali.

Il modello **multi-cloud** prevede l'**utilizzo simultaneo di servizi di cloud computing offerti da diversi provider pubblici**. Questa strategia permette di ottimizzare l'impiego delle risorse in base alle specifiche necessità aziendali, sfruttando le peculiarità dei vari fornitori come Amazon Web Services (AWS), Google Cloud Platform (GCP) e Microsoft Azure. L'adozione di un'architettura multi-cloud garantisce maggiore libertà di scelta ed evita la dipendenza da un singolo provider, riducendo il rischio di interruzioni del servizio.

I VANTAGGI DEL MULTI-CLOUD

- **Riduzione dell'infrastruttura on-premise:** le aziende possono esternalizzare carichi di lavoro, minimizzando i costi operativi e migliorando la scalabilità e l'efficienza.
- **Maggiore resilienza e continuità operativa:** la diversificazione tra più fornitori riduce il rischio di downtime e la vulnerabilità agli errori di un singolo provider.
- **Innovazione accelerata:** ogni provider offre soluzioni specifiche per l'intelligenza artificiale (IA), analisi dei dati e machine learning (ML), consentendo un rapido sviluppo di nuove funzionalità.
- **Svincolarsi dal vendor lock-in:** adottando più fornitori, le aziende mantengono flessibilità nella gestione dei servizi cloud e riducono la dipendenza da un unico provider.
- **Ottimizzazione dei costi:** la possibilità di confrontare i prezzi e le offerte di diversi fornitori consente di ridurre i costi operativi complessivi.

Vantaggi che hanno una notevole attrattiva sulle aziende. Prova ne è che, secondo l'indagine *"Cloud evolution: mandate to modernize"* effettuata da **HCL Tech** a livello globale nella seconda metà del 2024, l'**87% delle organizzazioni che opera in cloud utilizza più di un fornitore di servizi**, con una media di tre fornitori nella propria strategia multi-cloud. Inoltre, il 73% delle aziende dichiara di avere riorganizzato le applicazioni durante la migrazione al cloud, evidenziando un passaggio verso la modernizzazione cloud-native.

Scelte che hanno portato risultati rilevanti: l'83% delle aziende che collabora con consulenti terzi evidenzia un miglioramento dell'efficienza IT e delle prestazioni delle applicazioni. Al punto che gli intervistati sostengono che oggi è 2,2 volte più proba-

LEGGI L'INDAGINE DI HCL TECH

bile che le aziende adottino una strategia multi-cloud rispetto a tre anni fa. Come diretta conseguenza, e in linea con l'evoluzione tecnologica, il 93% del campione indica di stare esplorando soluzioni personalizzate di intelligenza artificiale generativa per poterle integrare nelle proprie strategie cloud.

Il **Rapporto 2024 di Flexera** sullo stato del cloud mostra un'adozione del multi-cloud in linea con quella rilevata da HCL Tech.

LEGGI IL CLOUD COMPUTING TRENDS: FLEXERA 2024 STATE OF THE CLOUD REPORT

Precisa però che le due principali implementazioni multi-cloud sono app isolate su cloud diversi e disaster recovery/failover tra cloud. Le app isolate su cloud hanno avuto l'incremento maggiore (fino al 57% dal 44% nel confronto anno su anno). Nel medesimo periodo, l'integrazione dei dati tra cloud è aumentata dal 37% al 45%, poiché le organizzazioni hanno cercato la soluzione migliore per applicazioni e analisi dei dati. Seguono l'integrazione dei dati tra cloud differenti (45%), lo spostamento di workload tra più cloud (40%) e la suddivisione delle applicazioni tra cloud pubblico e privato (35%).

La sfide del multi-cloud

Agli innegabili vantaggi che può apportare il multi-cloud, si associano però sfide altrettanto rilevanti:

- **Complessità gestionale:** monitorare e orchestrare servizi di diversi provider richiede strumenti avanzati di gestione e competenze specifiche per garantire un'efficace governance dei dati.
- **Conformità e sicurezza:** la gestione di dati su più piattaforme aumenta le criticità legate alla protezione delle informazioni e al rispetto delle normative locali e internazionali.
- **Costi variabili:** la gestione di un ambiente multi-cloud necessita di un'ottimizzazione costante per evitare spese impreviste e garantire una gestione efficiente delle risorse.
- **Interoperabilità limitata:** i servizi cloud non sono sempre compatibili tra loro, e la migrazione tra diversi ambienti può risultare complessa.

Hybrid cloud: pubblico e privato insieme per aumentare il controllo

L'hybrid cloud combina risorse di cloud pubblico e privato, consentendo alle aziende di mantenere il controllo sui dati sensibili e, al tempo stesso, beneficiare della scalabilità del cloud pubblico. Questa architettura è particolarmente vantaggiosa per settori regolamentati che necessitano di rispettare rigidi standard di conformità e sicurezza dei dati.

I VANTAGGI DEL HYBRID CLOUD

- **Sicurezza avanzata e conformità:** le informazioni critiche possono essere gestite su infrastrutture private, riducendo i rischi legati alla sicurezza e rispettando le normative di settore.
- **Scalabilità flessibile:** le risorse del cloud pubblico possono essere integrate per gestire picchi di lavoro senza compromettere le performance complessive.
- **Migliore controllo dei costi:** l'adozione di un mix di cloud consente di ottimizzare le spese in base ai requisiti operativi, minimizzando il rischio di sovrainvestimenti in infrastrutture IT.
- **Elevata disponibilità:** la combinazione di ambienti pubblici e privati garantisce la continuità operativa anche in caso di guasti o interruzioni di servizio.
- **Flessibilità operativa:** le aziende possono mantenere una parte delle operazioni su infrastrutture private e sfruttare il cloud pubblico per espandere rapidamente le risorse.

I dati raccolti dall'Osservatorio del Politecnico di Milano mostrano che il comparto public & hybrid cloud si conferma il principale motore della crescita, con una spesa di 4,8 miliardi di euro (+30% rispetto al 2023). Di particolare rilievo il sorpasso storico dei servizi **Infrastructure as a service (IaaS)** sui **Software as a service (SaaS)**, che tradizionalmente hanno dominato gli investimenti delle imprese. L'IaaS ha raggiunto il valore di 2,1 miliardi di euro (+42%), con una domanda in forte espansione per le virtual machine destinate a sviluppo, test e produzione.

La crescita è sostenuta anche dal **Platform as a service (PaaS)**, che segna un incremento del 23% (845 milioni di euro), spinto dall'adozione di modelli di IA come i **Large language models (LLM)** accessibili via API. Parallelamente, il SaaS si attesta a 1,8 miliardi di euro (+21%), con una crescente integrazione di funzionalità IA nei software di gestione documentale e collaborazione.

Sfide dell'hybrid cloud

Nonostante la crescita sostenuta, le imprese si trovano ad affrontare sfide significative nella gestione dell'hybrid cloud. Tra queste troviamo:

- **Integrazione complessa:** garantire un'interoperabilità efficace tra i diversi ambienti richiede investimenti in strumenti di gestione avanzati e risorse IT specializzate.
- **Latenza e prestazioni:** il trasferimento di dati tra cloud pubblici e privati deve essere ottimizzato per evitare colli di bottiglia e garantire tempi di risposta efficienti.
- **Gestione delle competenze:** l'adozione di un hybrid cloud richiede un team IT con conoscenze specifiche su ambienti distribuiti e piattaforme cloud.
- **Sicurezza dei dati:** la trasmissione di informazioni tra ambienti pubblici e privati necessita di robuste misure di crittografia e autenticazione per prevenire violazioni.

Il report dell'Osservatorio del Politecnico precisa che il 58% delle grandi organizzazioni segnala difficoltà nel controllo della spesa, mentre il 54% denuncia una carenza di competenze specializzate e il 43% evidenzia criticità nella gestione della sicurezza.

DINAMICHE DI ADOZIONE DEL CLOUD

Mentre le grandi aziende continuano ad accelerare nella migrazione al cloud, le piccole e medie imprese (PMI) mostrano un approccio più cauto. Secondo l'Osservatorio del Politecnico di Milano, il tasso di adozione rimane stabile al 67%, ma la spesa in public & hybrid cloud segna comunque un aumento del 21%, raggiungendo i 581 milioni di euro.
Nel contesto delle grandi organizzazioni, l'84% ha già migrato almeno parte dei dati critici in cloud, mentre solo il 2% ha intrapreso operazioni di repatriation, riportando dati e applicazioni su infrastrutture on-premise. Secondo i ricercatori dell'Osservatorio del Politecnico, le aziende italiane stanno acquisendo una crescente consapevolezza nell'adozione del cloud, adottando modelli cloud native e rivedendo scelte passate attraverso refactoring architetturali. Tuttavia, la trasformazione è ancora in corso e richiede una continua revisione delle strategie per sfruttare le nuove soluzioni offerte dai cloud provider, in particolare nel segmento SaaS e AI.

Uno non esclude l'altro

Nel contesto della trasformazione digitale, le architetture cloud stanno evolvendo rapidamente, offrendo alle aziende una varietà di opzioni per ottimizzare le proprie risorse IT. Spesso multi-cloud e il hybrid cloud vengono confusi tra loro e i loro nomi sono usati in modo intercambiabile. Tuttavia, presentano differenze sostanziali che influenzano la scelta strategica.

Il cloud ibrido è un sottoinsieme del modello multi-cloud. Un'infrastruttura multi-cloud si compone di diverse piattaforme cloud, ciascuna destinata a fornire applicazioni o servizi specifici. Al contrario, un'architettura di cloud ibrido integra risorse IT on-premises (infrastruttura fisica tradizionale o private cloud) con soluzioni di IaaS o altri servizi cloud pubblici forniti dagli hyperscaler o altri provider.

Un equivoco comune è che hybrid cloud e multi-cloud si escludano a vicenda. In realtà, un ambiente ibrido può essere considerato parte del multi-cloud, ma non tutte le configurazioni multi-cloud sono ibride.

Mentre il multi-cloud può includere più cloud pubblici senza necessariamente integrarli, il cloud ibrido richiede che esista un livello di interconnessione e interoperabilità tra le componenti on-premise e i servizi cloud pubblici.

La decisione tra multi-cloud e hybrid cloud dipende dagli obiettivi aziendali, dai requisiti di sicurezza e dalla necessità di flessibilità. Mentre il multi-cloud offre massima libertà di scelta, resilienza e innovazione, l'hybrid cloud garantisce maggiore controllo sui dati sensibili e conformità normativa.

Indipendentemente dall'opzione scelta, è fondamentale si usino strumenti di gestione avanzati per ottimizzare la governance e la sicurezza dell'infrastruttura cloud. Le aziende devono considerare le proprie necessità operative, le capacità di gestione IT e i costi complessivi prima di adottare una strategia cloud. La scelta ottimale sarà quella che meglio si allinea agli obiettivi di crescita e digitalizzazione dell'impresa, assicurando scalabilità, efficienza e competitività nel lungo periodo.

E in tale scelta un ruolo essenziale lo riveste il partner, che, oltre ad aiutare il cliente a implementare la soluzione migliore, inizia con l'azienda un percorso destinato a durare nel tempo.

Image: Freepik

Open Source, il motore della trasformazione digitale

Oggi è un pilastro fondamentale nelle infrastrutture IT delle aziende che ne riconoscono il ruolo chiave nell'accelerare l'innovazione. Non è più solo una alternativa economica, ma è un vantaggio competitivo per chi lo sceglie

di **Maurizio Ferrari**

L'open source è diventato grande; da nicchia per nerd è cresciuto fino a diventare un pilastro delle infrastrutture IT nel mondo enterprise. Oggi non ha più l'aura del garage con gli sviluppatori che creano e condividono codice, da diverso tempo non è più così. Oggi, parlare di open source significa parlare del cuore del mondo IT, un cuore fatto di codici ed esperienze condivise che impattano su tutti gli ambiti del business, spesso incentivati anche dalle normative che promuovono l'adozione di soluzioni open source nel settore della pubblica amministrazione e non solo. A sottolinearne l'importanza è **Emanuele Caronia, CEO di Exelab**, system integrator romano: *"L'open source è un pilastro della trasformazione digitale aziendale. L'evoluzione dei modelli di sviluppo basati su AI e analisi dei dati ha reso le tecnologie open un acceleratore strategico: framework come TensorFlow e PyTorch alimen-*

tano l'innovazione in ambiti chiave, mentre iniziative come DeepSeek dimostrano come anche nel settore degli LLM l'open source possa competere con soluzioni proprietarie. Questa evoluzione rappresenta un'opportunità e una sfida per gli operatori ICT. Opportunità, perché la trasparenza e la flessibilità dell'open source consentono di sviluppare soluzioni personalizzabili, riducendo il rischio di lock-in tecnologico. Tuttavia, la crescente complessità delle infrastrutture richiede un approccio strutturato alla governance e alla sicurezza. Secondo ***Kpmg, il 78% delle aziende utilizza componenti open source senza adeguati processi di monitoraggio****, aumentando il rischio di vulnerabilità nella supply chain del software. Le imprese che vogliono trarre il massimo dall'open source devono coniugare agilità e sicurezza, adottando strategie come la mappatura delle dipendenze software, l'automazione degli aggiornamenti e l'integrazione con framework di threat intelligence. In un mondo in cui velocità e affidabilità sono cruciali, l'open source non è solo una scelta tecnica, ma un vantaggio competitivo da gestire con visione e responsabilità".*

Anche per **Massimiliano Battaglia, product manager di VEM Sistemi**, l'open source è più che una soluzione per ridurre i costi delle licenze: *"Se in passato era considerato un modo per contenere i costi di licenza, oggi rappresenta un motore di sviluppo in diversi settori strategici, quali l'intelligenza artificiale, il cloud computing e la cybersecurity. L'integrazione con i modelli di sviluppo DevOps e Infrastructure as Code (IaC) ha reso l'open source un acceleratore di automazione ed efficienza operativa.*

L'APPROFONDIMENTO DI BIZZIT

L'INEVITABILE SCELTA DELL'OPEN INNOVATION

Uno studio Capgemini offre uno spaccato importante di cosa è oggi e soprattutto sarà nei prossimi anni il ricorso delle imprese a ecosistemi di innovazione per reggere la complessità competitiva. Crederci, con investimenti e trasformazioni di processo e culturali verso un'integrazione vera, rappresenta l'unica via per raggiungere flessibilità e capacità di reggere le disruption.

LEGGI QUI

Tuttavia, ogni evoluzione implica nuove sfide: una di queste è la gestione della sicurezza. Per cogliere le opportunità e al contempo mitigare i rischi, gli operatori del mondo ICT possono adottare diverse misure: in primo luogo, investire in soluzioni di sicurezza e conformità, come tecnologie di automated security scanning, strumenti di gestione della Software bill of materials (Sbom) e l'adozione di un approccio zero trust. Inoltre, la gestione efficiente di infrastrutture complesse richiede strumenti avanzati di observability e monitoraggio, che garantiscano un controllo proattivo sulle performance e la sicurezza delle architetture. Infine, la partecipazione attiva delle aziende alle community open source, contribuendo ai progetti chiave, rappresenta un'occasione per indirizzarne gli sviluppi e garantire un vantaggio competitivo duraturo".

Secondo **Massimiliano Bellifemine, responsabile della digital factory cloud & data driven applications di Exprivia**, l'importanza dell'open source nelle aziende è in costante aumento: *"Oggi è diventato essenziale in infrastrutture complesse e progetti innovativi, con un'adozione crescente da parte di aziende di ogni settore. Piattaforme open source come Kubernetes, TensorFlow e Apache Kafka sono esempi significativi di strumenti che permettono di attuare la trasformazione digitale, rispondendo a esigenze sempre più avanzate in termini di rapidità e scalabilità. Oggi l'open source si distingue anche per il suo* ***approccio collaborativo e agile****, e favorisce la rapida disponibilità di piattaforme e strumenti. Nel contesto degli operatori ICT, l'open source è una risorsa strategica per ottimizzare i costi, migliorare l'agilità operativa e introdurre innovazione e sperimentazione in modo rapido ed efficace. La flessibilità dell'open source consente alle aziende di* ***personalizzare le soluzioni e di integrarle nelle infrastrutture esistenti****. Tuttavia, questa evoluzione pone anche importanti sfide: la sicurezza e l'affidabilità rimangono temi critici. Per affrontarle è necessario adottare un approccio integrato che operi su più fronti: stringere partnership con le community open source, investire in formazione continua e utilizzare strumenti avanzati per la gestione delle vulnerabilità e delle infrastrutture. Questo approccio consente di mitigare i rischi e trasformare le criticità in opportunità per distinguersi sul mercato. L'open source non è più solo una tec-*

nologia: è un vero e proprio paradigma che guida l'evoluzione del settore ICT (e non solo). Le aziende che sapranno coglierne appieno le potenzialità potranno ottenere vantaggi concreti e competitivi".

Anche per **Jacopo Nardiello, head of cloud native services & open source di ReeVo**, siamo di fronte a un cambio di paradigma grazie all'evoluzione dell'open source: *"L'open source non è più solo condivisione di codice, ma rappresenta un modello di innovazione collaborativa che accelera lo sviluppo tecnologico. Progetti come Kubernetes dimostrano come le community open source possano creare standard de facto per interi settori. Allo stesso tempo, l'emergere di* ***progetti AI open source sta democratizzando l'accesso a tecnologie trasformative***, *ridefinendo il panorama tecnologico. Per gli operatori ICT, questo significa ripensare le strategie di sviluppo in un'ottica di collaborazione e contribuzione. Il vantaggio competitivo non deriva più dal codice proprietario, ma dalla capacità di integrare, orchestrare e innovare su basi open source. La sfida principale è trovare il giusto equilibrio tra apertura e sicurezza, implementando pratiche di sicurezza all'interno dei propri processi di sviluppo. La complessità crescente delle moderne infrastrutture IT richiede un nuovo approccio strategico: l'adozione di architetture cloud-native e dei principi open source diventa fondamentale per garantire agilità operativa e innovazione continua"*.

Anche **Luca Balzola, CTO di Exclusive Networks Italia**, è d'accordo e sottolinea il ruolo centrale dell'open source nel futuro delle ICT: *"L'open source è un passaggio chiave per gli operatori del settore e rappresenta un valore aggiunto per i servizi gestiti in ambito ICT e cyber sicurezza, grazie alla sua flessibilità, trasparenza e capacità di innovazione. L'integrazione di strumenti open source nei servizi a valore permette agli operatori di offrire soluzioni più personalizzabili, scalabili e competitive. Inoltre, la collaborazione con la community open source garantisce aggiornamenti continui e una risposta più rapida alle minacce informatiche, aumentando così l'efficacia e la qualità dei servizi offerti ai clienti. Questo approccio consente anche di accelerare il time-to-market e di ridurre i*

costi. Ancora più importante è la sua capacità di personalizzazione: l'open source non è più da considerarsi una soluzione alternativa/economica, ma è diventata un elemento centrale che favorisce la collaborazione fra aziende leader di settore. Tuttavia, per poterla utilizzare in modo efficace sono necessari governance, sicurezza e investimenti mirati".

Romeo Scaccabarozzi, amministratore delegato di Axiante, mette a fuoco il ruolo dirompente che l'open source ha avuto e ha tuttora: *"Nato come movimento "ribelle" contro i modelli proprietari, è oggi essenziale:* ***il 70% del software moderno lo utilizza e il 90% delle aziende lo integra****, dal momento che offre vantaggi strategici a cominciare dalla riduzione dei costi di licenza e dall'aumento della flessibilità. Apertura, reciprocità e accesso sono i valori fondanti di questa tipologia di soluzioni. Per consolidarli, però, sono necessari investimenti e supporto ai manutentori. Garantire compensi e favorire connessioni tra sviluppatori è pertanto cruciale per rendere l'open source accessibile a una comunità più diversificata. In un mondo frammentato, le competenze per collaborare in modo asincrono con diversi gruppi e tecnologie verso un obiettivo comune diventeranno sempre più cruciali per sviluppare una tecnologia più accessibile e innovativa. L'open source incarna trasparenza e inclusività, attirando sviluppatori motivati dall'impatto sociale. Dal punto di vista economico, l'open source aiuta le aziende a ridurre costi e dipendenza dai fornitori, evi-*

L'INCHIESTA DI BIZZIT

LO SVILUPPO SOFTWARE È AGILE E ABBRACCIA IL CLOUD

Le metodologie utilizzate dai principali attori del mercato oggi sfruttano al meglio le caratteristiche che la tecnologia mette a disposizione fornendo in tempi rapidi soluzioni scalabili sicure e integrate. Per arrivare a trovare la soluzione migliore, in un momento così dinamico, dove non esiste una sola scelta, ma il panorama è veramente ampio, abbiamo chiesto ai principali attori di questo mercato qual è il loro approccio per fornire la miglior soluzione alle realtà italiane.

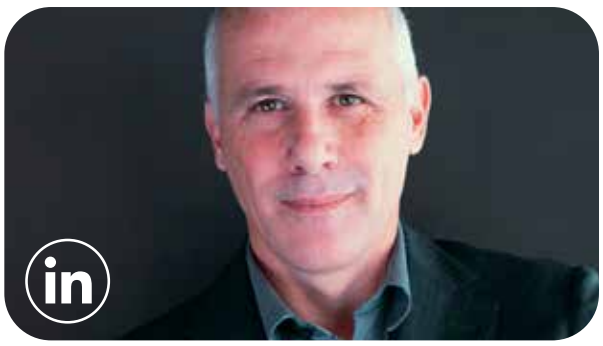
LEGGI QUI

tando il vendor lock-in. Abbassa inoltre le barriere all'ingresso per gli sviluppatori, democratizzando l'accesso alla tecnologia e offrendo strumenti gratuiti che favoriscono l'innovazione, come dimostra Python nel data science e nello sviluppo web. Tuttavia, la frammentazione dell'ecosistema complica la sicurezza, richiedendo competenze avanzate per gestire vulnerabilità e ridurre i rischi. Tuttavia, la forza dell'open source risiede proprio nella collaborazione: una comunità ampia può individuare e risolvere falle più velocemente. In questa direzione, standardizzare la sicurezza è essenziale per rendere l'ecosistema più sicuro e resiliente".

Marco Tessarin (nella foto a sinistra), presidente della RIOS (Rete italiana open source), e **Stefano Pampaloni, vice presidente** della stessa organizzazione, ci tengono a sottolineare che l'open source è oggi il motore dell'ICT e che risponde ai nuovi standard europei di questo settore: *"L'open source è passato da alternativa economica a pilastro strategico per le aziende e le pubbliche amministrazioni. Oggi è il motore dell'innovazione digitale, abilitando nuovi modelli di sviluppo e collaborazione. L'Europa impone nuovi standard con il Cyber resilience act (CRA) e l'AI Act, rendendo cruciale una gestione rigorosa del software open source e innalzando il livello dei servizi richiesti. Questa trasformazione rappresenta un'opportunità concreta per gli operatori ICT: superare la mera rivendita di soluzioni di terze parti significa costruire valore con competenze proprie. L'open source permette di sviluppare soluzioni personalizzate, creare prodotti differenziati e posizionarsi strategicamente. Per quanto riguarda la sicurezza, è fondamentale adottare strategie di security by design, con gestione delle dipendenze software (Sbom) e monitoraggio della conformità normativa. L'open source è il futuro del digitale, ma le sfide legate alla sicurezza, alla conformità normativa e alla gestione delle infrastrutture complesse richiedono competenze avanzate e una visione strategica. Il vero valore non risiede solo nell'adozione del software open source, ma nella capacità di svilupparlo, governarlo e renderlo sicuro. RIOS, grazie alla forza della sua rete, garantisce l'accesso a competenze di alto livello e supporta imprese, istituzioni e comunità nell'affrontare queste sfide con soluzioni concrete e*

sostenibili. Gli operatori ICT che investiranno in know-how e contribuiranno attivamente all'ecosistema open source potranno giocare un ruolo da protagonisti in un mercato sempre più competitivo e regolamentato".

IBM, nella figura di **Walter Aglietti, IBM technical leader manager**, mostra come business e open source possano coesistere: *"Coerente con i propri valori, IBM ha da tempo scelto l'open source come elemento fondante di tutta la sua offerta, dall'AI generativa, alla virtualizzazione, al quantum computing, con l'obiettivo di creare ecosistemi aperti e flessibili per la modernizzazione dell'IT senza vincoli per le aziende. In ambito AI, IBM ha sviluppato il proprio portafoglio WatsonX con un approccio aperto e trasparente, seguendo linee guida etiche e valoriali condivise con la comunità open source. Inoltre, la famiglia dei modelli IBM Granite viene rilasciata anche come open source e la metodologia InstructLab, creata da IBM e Red Hat, consente di risparmiare tempo e risorse nella fase di addestramento e di sviluppare modelli di base attraverso una serie di contributi incrementali che migliorano le soluzioni senza l'uso di tecnologie proprietarie. Questo metodo permette di lavorare in modalità multi-modello e multimodale e di adottare anche modelli di terze parti con libertà. IBM è inoltre tra i promotori dell'AI Alliance, un'organizzazione che sostiene la collaborazione tra aziende, istituzioni, ricercatori e accademia per lo sviluppo governato dell'AI con un approccio condiviso. IBM adotta una strategia open source anche per quanto riguarda le tecnologie di virtualizzazione e orchestrazione, dove promuove ecosistemi aperti attraverso progetti come OpenShift e KVM. Questo permette di ottenere soluzioni scalabili e flessibili, sia su infrastrutture on-premise che su cloud ibridi, e si differenzia radicalmente dagli approcci proprietari. È così che IBM risponde alle esigenze di modernizzazione delle infrastrutture aziendali, guidando l'innovazione in modo sostenibile e trasparente".*



Roberto Vicenzi, chief sales and marketing officer di MegaByte, pone l'accento su alcuni aspetti della filosofia open source, con un focus particolare sulla sicurezza: *"I recenti episodi di sicurezza, come l'incidente CrowdStrike del 2024,*

hanno messo in luce l'importanza della trasparenza del codice e della sicurezza partecipativa, caratteristiche tipiche dell'open source. La nostra esperienza con Proxmox dimostra che le moderne soluzioni open source offrono vantaggi competitivi significativi. Oltre alla riduzione dei costi (fino all'80% rispetto a soluzioni proprietarie come VMware), l'open source garantisce un maggiore controllo, flessibilità e indipendenza dai fornitori. Gli operatori ICT possono ottimizzare le proprie strategie puntando su: trasparenza e sicurezza; innovazione collaborativa, sviluppo guidato da esigenze reali degli utenti; scalabilità, adattamento rapido alle necessità aziendali; indipendenza tecnologica, nessun vendor lock-in. La gestione di infrastrutture complesse richiede competenze specializzate. Noi di MegaByte affianchiamo i nostri clienti nell'adozione di soluzioni open source enterprise-ready come Proxmox, garantendo supporto certificato e integrazione con l'hardware esistente. L'open source rappresenta oggi la scelta strategica per un'infrastruttura IT moderna, sicura ed economicamente efficiente, specialmente nell'era dell'intelligenza artificiale e dell'iperconvergenza. Innovare significa crescere: le nuove soluzioni offrono sempre vantaggi concreti alle imprese".

Red Hat, nella figura di Rodolfo Falcone, country manager Italy, evidenzia il ruolo di assoluta protagonista che la filosofia open source riveste in questo momento storico: *"I vantaggi promessi dall'AI sono sotto gli occhi di tutti e non sarebbero possibili senza la possibilità di accedere a piattaforme open source e condividere dati e competenze. Comprensibilmente, l'interesse del mercato è alto, come dimostrano le 4000 presenze registrate ai Red Hat Summit Connect di Roma e Milano, solo qualche mese fa. In quell'occasione, aziende e organizzazioni di grande prestigio hanno illustrato al pubblico come le piattaforme open source enterprise di Red Hat abbiano reso possibili progetti di innovazione e digitalizzazione di grande impatto. Oggi, le più importanti infrastrutture al mondo, in ogni settore, si basano su piattaforme open source. I vantaggi per gli operatori ICT, ma anche per i clienti finali, sono molteplici, a cominciare dalla possibilità di garantirsi* ***prestazioni elevate abbinate a una flessibilità*** *senza eguali. Altri elementi di rilievo sono la spinta innovativa della community e l'indipendenza dai vendor, soprattutto in*

L'APPROFONDIMENTO DI BIZZIT

OPEN INNOVATION: PILASTRO STRATEGICO PER LE IMPRESE MODERNE

Le aziende puntano sempre più sull'open innovation collaborando con partner esterni. Per rimanere competitive, devono costantemente aggiornare processi, tecnologie e competenze interne, rendendo l'innovazione condivisa una priorità strategica.

Una manifestazione concreta di open source.

LEGGI QUI

momenti di incertezza geopolitica come quelli che stiamo vivendo. Per amplificare gli effetti positivi dell'open source, le aziende devono adottare un approccio strategico, investendo in competenze e collaborando con la community, considerando con la dovuta attenzione gli aspetti più delicati, quali la sicurezza e la complessità delle infrastrutture. In questo senso, l'apertura e l'interoperabilità tipiche delle piattaforme open source, abbinate all'approccio enterprise offerto da Red Hat, hanno un valore inestimabile come abilitatori dell'innovazione".

Secondo **Galina Godukhina, sales director di Onlyoffice**, l'open source offre una serie di vantaggi unici che permettono di ottenere un vantaggio competitivo: *"Oggi, i modelli ibridi combinano trasparenza e supporto premium, mentre l'integrazione con l'AI accelera lo sviluppo. Onlyoffice ne è un esempio: offre strumenti open source per la produttività aziendale con AI Assistant per ottimizzare la gestione documentale. Gli operatori ICT possono trarre vantaggi e ottimizzare le strategie aziendali grazie a: flessibilità e indipendenza, riduzione dei costi, innovazione continua, sicurezza avanzata, intelligenza artificiale e automazione, riduzione dei tempi per le attività quotidiane. Le sfide non mancano: la governance, la sicurezza e la gestione infrastrutturale richiedono strategie solide, ma con strumenti come Onlyoffice, l'open source diventa una scelta strategica per ottimizzare i processi e innovare il business".*

Compliance normativa: ecco le leggi che regolano il digitale

Adeguarsi a normative che sono in continua evoluzione per tenere il passo con l'evoluzione tecnologica pone sfide complesse, perché ci si deve adattare a requisiti stringenti senza compromettere l'innovazione ed effettuare investimenti in sicurezza, governance dei dati e formazione del personale

di **Fabrizio Pincelli**

La tecnologia informatica sta evolvendo molto rapidamente e questo porta notevoli benefici, ma spesso per poter trarre un reale vantaggio da tali benefici è necessario imporre dei limiti affinché si abbia la certezza che non ci siano effetti collaterali negativi sulle persone, sulle imprese e anche sulla società civile. Tali limiti si traducono in normative che sono applicate ad ampio spettro, dalla cybersecurity all'efficienza, dal controllo delle emissioni all'archiviazione dei dati. Oggi chi opera nel mondo dell'ICT deve essere a conoscenza delle normative che regolano il settore, che molto spesso sono il recepimento di normative europee. Vediamo quali sono quelle con cui più spesso ci si deve confrontare.

La sicurezza IT, il settore più normato

L'ambito che per antonomasia deve avere delle regole è quello

della sicurezza. Oggi il problema della **cybersecurity** ha assunto una rilevanza tale che deve essere affrontato in modo strutturale, non basta più erigere una protezione basandosi su un software antivirus o un firewall.

Gli attacchi sono sempre più mirati e raffinati e gli obiettivi più strategici. Nel 2023 gli incidenti censiti dal **Clusit** sono aumentati dell'11% a livello globale rispetto al 2022 (ma quelli verso l'Italia hanno registrato addirittura un +65%). La tendenza globale del primo semestre 2024 mostra una ulteriore crescita, molto significativa, pari al 23% rispetto al semestre precedente. In media, si sono verificati nel mondo 9 attacchi importanti al giorno; in Italia il 7,6% degli incidenti. La **sanità è il settore più colpito** a livello globale. Nel nostro Paese il più bersagliato è il **settore manifatturiero** (19%), ma gli attacchi alla sanità sono cresciuti dell'83% rispetto al primo semestre 2023.

1° Manifacturing

il settore più colpito da incidenti cyber in Italia nel primo semestre 2024

Nell'88% dei casi gli attacchi sono perpetrati da cybercriminali che hanno come obiettivo principale l'ottenimento di denaro. Questo spesso avviene chiedendo un riscatto per consentire di poter di nuovo accedere ai dati "sequestrati", essenzialmente tramite malware/ransomware (34% dei casi) o phishing (8%), bloccando l'attività di un'azienda o di una struttura sanitaria. I danni che possono causare questi attacchi sono enormi.

NIS2, la cybersecurity secondo la UE

Per cercare di limitare questo problema a livello UE è stata istituita nel 2016 la direttiva **NIS (Network information security)**, con la quale sono state definite sia precise pratiche per la cybersecurity sia anche chi le deve adottare, in particolare strutture che si occupano di servizi essenziali. Dallo scorso 17 ottobre è in vigore la **NIS2**, versione corretta e attualizzata della direttiva, attraverso la quale la UE intende fare sì che le aziende che costituiscono il tessuto socioeconomico siano più affidabili riguardo la sicurezza IT. In tal senso, NIS2 amplia da alcune centinaia a decine di migliaia il numero delle aziende che devono adottare misure di protezione basate su un approccio che includa **politiche di analisi dei rischi, gestione degli incidenti, continuità operativa, sicurezza**

della supply chain e altre disposizioni. Inoltre, chiarisce le responsabilità del management aziendale e i tempi di notifica degli incidenti (le aziende devono segnale quelli significativi entro 24 ore). In più, obbliga il management all'attuazione e alla supervisione della conformità alla direttiva. La trasgressione può causare multe e, in casi gravi di non conformità, la sospensione temporanea dalle funzioni manageriali.

NIS2 ha un diretto impatto anche sugli operatori del mondo IT. Infatti, si estende alla **sicurezza della supply chain**, richiedendo alle aziende di valutare le vulnerabilità dei propri fornitori e di adottare misure correttive quando necessario.

Da sottolineare che lo **ISO 27001**, standard che guida alla messa in pratica delle best practice sulla sicurezza delle informazioni, può essere un valido framework per attuare quanto previsto dalla NIS2.

La legge italiana sulla cybersicurezza 90/24 (GU n. 153 del 2 luglio 2024) può essere considerata un adeguamento a quanto stabilito dalla NIS2 perché stabilisce precise *"disposizioni in materia di rafforzamento della cybersicurezza nazionale, di resilienza delle pubbliche amministrazioni e del settore finanziario, di personale e funzionamento dell'Agenzia per la cybersicurezza nazionale e degli organismi di informazione per la sicurezza nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici"*.

Legge 90/24

Regolamento Macchine, la sicurezza arriva anche nel manufacturing

Come detto, il manufacturing è il settore più colpito dai cybercriminali. Questo perché sempre di più le **macchine e le fabbriche sono connesse** e ciò comporta un'esposizione agli attacchi spesso favorita da **software che non sono adeguatamente protetti**. Così l'evoluzione tecnologica in ambito OT sta imponendo ai produttori una rapida revisione del loro modello di gestione dei rischi. Proprio per questo, nell'ottica di un comune approccio alla cybersecurity all'interno dei Paesi membri dell'UE, è stato emanato il Regolamento 2023/1230 (più noto come **Regolamento Macchine)**, in vigore da luglio 2023.

Come si legge nel rapporto Clusit, da tempo esistono standard consolidati per lo sviluppo di software strutturalmente solido, come ISO-5055 (che copre le aree relati-

ve alla sicurezza, all'efficienza, alla robustezza e alla manutenibilità), come peraltro esistono standard specifici per lo sviluppo di sistemi IoT, quali IEEE 2700-2017, IEEE P1451.99, IEEE P2020, IEEE P2520 e IEEE P2846. Tuttavia, sino a non molto tempo fa, l'aderenza a tali standard era lasciata all'iniziativa del singolo costruttore o del singolo system integrator. Il Regolamento Macchine tenta invece di rispondere all'esigenza di un riferimento comune per lo sviluppo di macchine e automazioni nelle quali le nuove tecnologie, come l'IoT, siano inserite rispettando determinati standard di qualità e sicurezza. Il software assume così un ruolo essenziale per la sicurezza delle macchine stesse. Questo comporta che, oltre al marchio CE, deve essere associata sia una dichiarazione di conformità UE nei confronti del Regolamento, sia istruzioni operative specifiche così da avere un'efficace gestione dei rischi potenziali cui potrebbero incorrere le macchine e le componenti IoT durante il funzionamento.

Regolamento DORA: la nuova resilienza digitale per la finanza

Per rafforzare la resilienza digitale nel settore finanziario, l'Unione Europea ha introdotto il 17 gennaio 2025 il **Regolamento DORA (Digital operational resilience act)**. Parte del Regolamento UE 2022/2554, DORA mira a garantire la continuità operativa di istituzioni e fornitori ICT, armonizzando le normative sulla cybersecurity.

DORA impone un framework uniforme per affrontare cyberattacchi, guasti tecnologici e vulnerabilità informatiche. Si applica a banche, assicurazioni, prestatori di servizi di pagamento, infrastrutture di mercato e fornitori ICT critici. Le aziende devono adottare strategie di gestione del rischio, segnalare tempestivamente gli incidenti di sicurezza e sottoporsi a test di resilienza, inclusi test di penetrazione avanzati. Inoltre, devono garantire la supervisione dei fornitori di servizi tecnologici e condividere informazioni sulle minacce emergenti. La mancata conformità comporta sanzioni severe e restrizioni operative. DORA rappresenta un cambio di paradigma nella sicurezza digitale del settore finanziario, imponendo standard elevati e vigilanza costante.

GDPR: la norma europea per la protezione dei dati

Un caposaldo dell'archiviazione nell'Unione Europea, entrato in vi-

gore il 25 maggio 2018, è il **Regolamento Generale sulla Protezione dei Dati (General data protection regulation - GDPR)**, che rappresenta una svolta fondamentale nella gestione della privacy e della sicurezza dei dati personali. Con un approccio basato sulla trasparenza, la responsabilizzazione e il controllo da parte degli utenti, la normativa impone rigorosi obblighi a tutte le organizzazioni che trattano dati di cittadini europei, indipendentemente dalla loro ubicazione geografica.

Uno dei principi chiave del GDPR è la **tutela dei diritti degli individui**, che possono richiedere accesso, modifica o cancellazione delle proprie informazioni personali. Le aziende sono tenute a raccogliere e trattare i dati solo per finalità esplicite e legittime, garantendo il rispetto del principio di minimizzazione e adottando misure di sicurezza adeguate e avendo l'obbligo di notificare eventuali violazioni entro 72 ore all'autorità di controllo competente. Inoltre, il regolamento introduce il concetto

IL CODICE PER INFORMATIZZARE LA PA

Riguardo la digitalizzazione della Pa italiana, va ricordato il ruolo del **Codice dell'Amministrazione Digitale (CAD)**: è infatti un testo unico che riunisce e organizzale norme riguardanti l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese. Questo significa, in pratica, che definisce che tutti i documenti amministrativi devono nascere informatici e devono essere trattati dalle Pa in un sistema affidabile di gestione documentale. Istituito nel 2005, nel tempo ha subito una serie di modifiche, per essere sia adattato alle evoluzioni tecnologiche sia razionalizzato nei contenuti. Oggi, tra l'altro, garantisce maggiore certezza giuridica alla formazione, gestione e conservazione dei documenti informatici prevedendo che non solo quelli firmati digitalmente - o con altra firma elettronica qualificata - ma anche quelli firmati con firme elettroniche diverse possano, a certe condizioni, produrre gli stessi effetti giuridici e disporre della stessa efficacia probatoria senza prevedere l'intervento di un giudice caso per caso. L'obiettivo è attribuire a cittadini e imprese i diritti all'identità e al domicilio digitale, alla fruizione di servizi pubblici online e mobile oriented, a partecipare effettivamente al procedimento amministrativo per via elettronica e a effettuare pagamenti online.

di portabilità dei dati, consentendo agli utenti di trasferire le proprie informazioni da un servizio all'altro senza impedimenti.

AI Act classifica l'intelligenza artificiale

Un discorso a sé va fatto per l'intelligenza artificiale, per la quale è stata definito l'**AI Act**. È una normativa europea che garantisce lo **sviluppo e l'uso sicuro dell'AI**, bilanciando innovazione e tutela dei diritti fondamentali. La crescente diffusione di sistemi di intelligenza artificiale in settori critici come sanità, finanza e sicurezza pubblica ha infatti reso necessaria l'introduzione di regole chiare per mitigare i rischi e assicurare la trasparenza nell'utilizzo di queste tecnologie.
Il regolamento classifica i sistemi di AI in base al livello di rischio, adottando un approccio basato sulla valutazione dell'impatto che queste tecnologie possono avere sugli individui e sulla società. Sono vietati i sistemi che presentano un livello di rischio inaccettabile per la sicurezza delle persone, come quelli utilizzati per definire una classificazione in base al comportamento sociale o alle caratteristiche personali. I sistemi considerati ad alto rischio, come quelli impiegati nella sorveglianza biometrica o nei processi di selezione automatizzata del personale, sono soggetti a requisiti stringenti in termini di trasparenza, governance e sicurezza. In particolare, il regolamento impone obblighi di conformità per garantire che l'AI sia sviluppata in modo etico, rispettando il principio di non discriminazione e l'affidabilità dei risultati. Meccanismi di sorveglianza, verifica e certificazione a livello europeo garantiscono che le applicazioni AI rispettino i requisiti normativi prima della loro immissione sul mercato.
Le autorità nazionali e un organismo UE di supervisione hanno il compito di monitorare l'applicazione del regolamento e sanzionare eventuali violazioni.
È stato sviluppato anche un **AI Act Compliance Checker** per aiutare le PMI e le startup a comprendere meglio se potrebbero avere obblighi legali ai sensi dell'AI Act o se potrebbero implementare l'Act solo per far risultare più affidabile la propria attività. Questo strumento può aiutare ad avere un'indicazione sugli obblighi che un sistema può dover affrontare-

Sostenibilità: le regole per limitare l'impatto ambientale del digitale

La crescente digitalizzazione e l'ampio ricorso al cloud (amentato anche in virtù dell'uso dell'AI) ha portato a un rilevante incremento del consumo energetico, richiedendo alle aziende l'adozione di soluzioni più sostenibili e conformi alle normative ambientali. Ricordiamo che nell'ottobre 2020 la Commissione Europea ha annunciato un pacchetto legislativo per ridurre entro il 2030 le emissioni di gas serra almeno del 55% e per realizzare una UE neutrale dal punto di vista climatico entro il 2050.

Uno degli strumenti normativi più rilevanti è la direttiva europea sulla **Rendicontazione di Sostenibilità Aziendale (Corporate sustainability reporting - CSRD)**, che obbliga le aziende a divulgare informazioni dettagliate sulle proprie strategie, politiche e azioni in ambito ESG (Environmental, social, governance), compresa la gestione dell'impatto digitale. Questa direttiva si integra con il regolamento sulla **Tassonomia UE**, che classifica le attività economiche sostenibili, volta a indurre le imprese IT a ridurre il proprio consumo di risorse e a implementare strategie di efficienza energetica.

Il settore IT è inoltre influenzato dal regolamento sulla **progettazione ecocompatibile dei prodotti sostenibili (Ecodesign for sustainable products regulation - ESPR)**. Entrato in vigore nel luglio 2024, stabilisce requisiti di progettazione, al fine migliorare significativamente la sostenibilità di tutti i prodotti immessi sul mercato dell'UE, potenziandone la circolarità, le prestazioni energetiche, la riciclabilità e la durabilità. Dal canto suo, l'**Energy efficiency directive (EED)** impone standard di efficienza per data center e infrastrutture digitali, obbligando le aziende a monitorare e ridurre il proprio impatto ambientale.

Anche normative ISO forniscono riferimenti chiave per la gestione ambientale e la sostenibilità IT. La **ISO 14001** definisce standard per la gestione ambientale aziendale, mentre la **ISO 50001** si concentra sulla gestione dell'energia, aiutando le imprese a ottimizzare i consumi nelle infrastrutture digitali.

I VANTAGGI DELLA COMPLIANCE PER GLI OPERATORI IT

I vendor e i loro partner sono i primi a dover aderire agli standard normativi. Lo devono fare in quanto aziende che operano in un settore normato come quello dell'IT, ma anche quali fornitori. Infatti, il controllo della supply chain ha assunto un ruolo centrale nelle strategie delle imprese di ogni dimensione.

Tuttavia, questa necessità può rivelarsi anche un'opportunità strategica. Infatti, la possibilità di dimostrare la compliance offre alcuni importanti vantaggi.

MAGGIORE COMPETITIVITÀ SUL MERCATO
le aziende conformi alle normative sono più affidabili agli occhi di clienti e investitori.

PIÙ FACILE ESPANSIONE VERSO NUOVI MERCATI
la compliance con normative internazionali consente di operare a livello globale senza limitazioni.

RIDUZIONE DEI COSTI LEGATI ALLE SANZIONI
evitare multe per il mancato rispetto delle normative è essenziale per una gestione economica sostenibile.

SICUREZZA DEI DATI RAFFORZATA
l'adozione di best practice per la protezione dei dati riduce il rischio di violazioni e attacchi informatici.

L’innovazione italiana passa dalla coesione in Europa

di **Leo Sorge**

La 2ª edizione del Rapporto Ricerca e Innovazione ICT in Italia, realizzato da Anitec-Assinform delinea lo scenario di un Paese competente ma in ritardo dal punto di vista tecnologico, che dovrebbe guardare alle sinergie nella partecipazione ai programmi europei. Ma forse non basta.

Piccoli, scoordinati e in ritardo, con personale scarso, scadente e in fuga dalla Patria e dalle aziende. Ma con qualità che, se finanziate modernamente e coese dentro l’Italia e dentro l’Europa, potrebbe dire la sua. Questo è il quadro dell’Italia tecnologica, a voler fare le pulci ai dati e a interpretarli guardando al futuro.

Piccoli nell’Unione europea (che già è piccola tra macroaree), disinformati sull’Europa e ormai obbligati al coordinamento nazionale ed europeo, in affannosa rincorsa tra la richiesta di un finanziamento, il tracciamento di Pmi e start-up e l’inseguimento delle competenze smarrite.

La 2ª edizione del **Rapporto Ricerca e Innovazione ICT in Italia**, realizzato da **Anitec-Assinform** in collaborazio-

SCARICA IL RAPPORTO RICERCA E INNOVAZIONE ICT IN ITALIA

di Anitec-Assinform

ne con Apre (l'Agenzia per la Promozione della Ricerca Europea), si pone l'obiettivo di fare dell'Italia *"un market maker e non un market taker"*, ha detto **Luisa Bordoni, responsabile dell'Ufficio Studi Anitec-Assinform**. Il quadro presentato è stato sì chiaro e dettagliato, ma purtroppo non attuale.

In una turbolenza che ormai sta diventando regola, con enormi cambiamenti sociali climatici o tecnologici e geopolitici, è opportuno chiedersi che senso abbiano analisi e decisioni basate su dati vecchi di oltre due anni, quelli del 2022. Non vuole essere questa una critica a chi questi dati li raccoglie e li analizza con precisione, ma esclusivamente la constatazione che l'Europa è in difficoltà se i tempi sono questi.

La situazione è stata dettagliata nell'ambito degli strumenti europei -Horizon 2020, partenariato, Pnrr e Ipcei- che insieme agli investimenti diretti e indiretti del settore pubblico fanno l'architettura di riferimento delle imprese europee. Rimandando in attesa del prossimo piano, il lontano **FP10:** il decimo programma quadro di ricerca e innovazione dell'UE, che dovrebbe entrare in vigore dopo la conclusione di Horizon Europe (2021-2027). Di qui e di là sono stati citati le start-up verso lo scale-up (ma non la recente revisio-

R&S A LIVELLI PRE-PANDEMIA

Nel 2022, la spesa per R&S *intra-muros* nel settore ICT ha raggiunto quota 2,5 miliardi di euro, con una crescita minima nel 2021 (1,5%). Quasi la metà di questi due miliardi e mezzo si è concentrata nel settore del software e dei servizi IT, mentre le aziende di produzione di hardware hanno registrato un aumento del 7,1% rispetto all'anno precedente. L'84% degli investimenti in Ricerca e Sviluppo nel settore ICT è arrivato da fondi privati, a dimostrazione del forte impegno delle aziende italiane nell'innovazione tecnologica. Gli addetti coinvolti in attività di R&I sono 52.000 e quasi 19.600 i ricercatori a tempo pieno.

HORIZON

Il Rapporto sottolinea che l'Italia ha ricevuto complessivamente 724,1 milioni di euro attraverso il programma Horizon 2020 per progetti di R&I ICT e, a fine 2024, 293,2 milioni di euro attraverso Horizon Europe. Il tasso di successo è in aumento rispetto al passato, ma ancora inferiore a Germania e Francia. La quota di spesa R&S intra-muros nel settore ICT per l'Italia è scesa dal 9,5% al 6,7% della spesa complessiva dell'UE27 tra il 2010 e il 2022: l'Italia soffre ancora di un sottodimensionamento rispetto alle maggiori economie europee.

ne della normativa) e la rilevanza dei dati, del loro impiego, della brevettabilità e delle leggi relative.
Al di là degli interventi istituzionali, più o meno rilevanti, è stata utile la presenza di due dirigenti dei ministeri centrali per lo sviluppo, il **Miur** (ricerca) e il **Mimit** (innovazione).
"Abbiamo adottato il metodo quantum, mettendo insieme tutti gli operatori in una stanza: mai prima Miur, Mimit, Acn e altri avevano dialogato così tanto", ha detto **Francesca Galli, dirigente ufficio di gabinetto del Miur**. *"Bisogna adottare anche altrove il metodo quantum* - le fa eco **Luca De Angelis, direttore generale tecnologie abilitanti al Mimit** - *che funziona e inoltre aumenta le percentuali di successo. Tra i vari meccanismi d'innovazione grande risalto devono avere gli Ipcei, Importanti progetti di comune interesse europeo, che sono tre: microelettroniche, intelligenza artificiale ed Edge. L'Italia è un mercato troppo piccolo per avere un'economia di mercato tutta sua e quindi dobbiamo fonderci con altre realtà ovviamente a partire dall'Europa". "Bassa natalità, migrazione dei cervelli., riduzione della durata delle competenze",* ha poi aggiunto **Francesco De Santis, VP R&S Confindustria**. *"Attenzione a tutto il ciclo di vita del dato, fino all'uso* - ha sottolineato **Valentino Valentini, vice ministro Mimit**, aggiungendo che per adeguare i finanziamenti - *serve un mercato europeo dei capitali unico, cinque diversi non vanno bene"*.

Le 4 misure proposte

Cosa fare dunque per rafforzare il ruolo dell'Italia nella Ricerca e Innovazione ICT e migliorare la competitività del Paese di fronte alle sfide tecnologiche che si prospettano a livello globale? Il Rapporto Anitec-Assinform suggerisce 4 misure: più sinergie nella **partecipazione ai programmi europei e Pnrr**, **maggior credito d'imposta** per la R&I ICT, **un modello a rete** per la ricerca applicata e il **rafforzamento del capitale umano**.
Sinceramente i quattro punti proposti da Anitec-Assinform non sembrano attuali, né attualizzabili. Difficilmente il credito d'imposta potrà portare risultati affidabili nella tecnologia avanzata.
È invece centrale, a nostro avviso, il richiamo di tutti a una vera collaborazione sinergica e se vogliamo anche dell'auspicio -scritto nel **Piano Draghi** - di rendere strutturali gli investimenti europei finora

SU BIZZIT

DRAGHI E IL DRAGONE: BASTERÀ ALL'EUROPA UN CHIPS ACT 2.0?

LEGGI QUI

straordinari, nonostante ciò che potrebbe voler dire per il mondo della Finanza. Tecnologia e geopolitica avanzano senza trattative e l'Europa non è adeguatamente dotata di infrastrutture tecnologiche sufficientemente avanzate e resilienti né sarà in grado di risolvere questo problema nell'immediato futuro.

Preparandosi al quantum computing

La seconda parte del Rapporto offre un'analisi dettagliata del settore emergente delle **quantum technologies**, evidenziando il loro potenziale rivoluzionario e la loro centralità per l'evoluzione del digitale. L'argomento è interessante, oltre che adatto alle competenze in fisica dell'Italia. Anche in questo caso, però, il commento potrebbe essere scritto senza leggere il rapporto.

Pur avendo un crescente impegno in questo settore grazie al Pnrr, l'Italia è ancora indietro rispetto a Stati Uniti e Cina (non solo in termini di investimenti e produttività brevettuale).

Per competere a livello globale nella corsa allo sviluppo di nuovi mercati di tecnologie e componenti quantistiche, l'Italia deve aumentare da milioni a miliardi gli investimenti per il Quantum attraverso ricerca applicata, protezione brevettuale e sviluppo di ecosistemi di innovazione che integrino ricerca avanzata ed esigenze industriali.

Ovviamente questa cosa non è possibile in tempi brevi. Ciononostante, la foto del mondo **quantum italiano** presente nel Rapporto è dettagliata, interessante e comprensibile: ne raccomandiamo la lettura a tutti gli interessati, anche perché in questo caso i dati sono sufficientemente recenti.

Anche in questo caso il rapporto Anitec-Assinform suggerisce una serie di politiche chiave per accelerare lo sviluppo e l'adozione di queste tecnologie. Sono molto qualitative: **aumentare l'interesse generale verso il quantum, prepararsi a nuovi scenari di rischio cyber, creare una solida base di competenze quantistiche.** Mentre ci chiediamo quanto siamo preparati alle competenze del futuro, nelle scuole medie italiane si riaffaccia il latino. Anche in questo caso viene da chiedersi quanto siamo pronti, parati in quella antica lingua, alle conseguenze.

Immagine di Freepick

Agenti AI tutti li vogliono

Secondo il Connectivity Benchmark Report di MuleSoft il 96% delle aziende europee punta sugli agenti AI per migliorare efficienza e produttività, ma l'integrazione dei dati si conferma come la sfida chiave per ottenere il massimo da questa tecnologia

di **Maurizio Ferrari**

L'intelligenza artificiale (AI) sta cambiando il modo in cui le aziende operano, offrendo nuove opportunità di automatizzare i processi, migliorare l'efficienza e ridurre i costi. Tuttavia, per poter adottare su larga scala gli **agenti AI**, ossia sistemi autonomi in grado di prendere decisioni e agire in base ai dati, è necessaria una solida infrastruttura di integrazione dei dati. Secondo il **10° Connectivity Benchmark Report di MuleSoft**, il 69% delle aziende europee identifica l'**integrazione dei dati** come una delle principali sfide nell'adozione dell'AI. Il rapporto, basato su

INTEGRAZIONE DATI COME OSTACOLO

69%

Aziende europee che considera l'integrazione dei dati come ostacolo per l'implementazione AI

un'indagine condotta su 1.050 leader IT in tutto il mondo, offre una panoramica dettagliata sullo stato attuale dell'adozione dell'AI e sulle barriere che le aziende devono superare per sfruttarne appieno il potenziale.

Agenti AI in crescita

Il 96% dei responsabili IT delle aziende europee ha già implementato o prevede di implementare agenti AI nei prossimi due anni. Questi sistemi, progettati per agire autonomamente, **raccolgono dati strutturati e non strutturati** da fonti come CRM, ERP, e-mail, PDF e Slack, supportando i team IT e migliorando l'efficienza operativa.

Tuttavia, **solo il 32% delle applicazioni è attualmente connesso** all'interno delle aziende europee, un dato che limita significativamente l'accuratezza e l'utilità degli agenti AI.

Il 94% degli intervistati ha dichiarato di avere difficoltà a integrare i dati tra i vari sistemi. Questo problema è particolarmente rilevante per le aziende che utilizzano agenti AI, dove il 91% dei dirigenti IT segnala che i silos di dati ostacolano significativamente il loro lavoro. Le aziende europee utilizzano in media 789 applicazioni, mentre quelle che sfruttano agenti AI ne utilizzano addirittura 1.075. Tuttavia, la mancanza di integrazione tra queste applicazioni limita la capacità degli agenti AI di operare in modo efficace, riducendo il loro impatto sulla produttività e sull'efficienza.

Più produttività nel futuro

Nonostante le sfide, **il 92% dei responsabili IT europei ritiene che l'AI aumenterà la produttività** dei propri sviluppatori nei prossimi tre anni. Tra le aziende che già utilizzano agenti AI, questa percentuale sale addirittura al 98%. Gli agenti AI offrono l'opportunità di automatizzare compiti ripetitivi e complessi, liberando risorse IT da dedicare ad attività a maggior valore aggiunto. Tuttavia, per raggiungere questo obiettivo, è essenziale **risolvere i problemi di integrazione** e garantire che gli agenti AI abbiano accesso a dati accurati e aggiornati.

PRODUTTIVITÀ

92%

Responsabili IT europei che ritiene che l'AI aumenterà la produttività

API per agenti AI più performanti

Le **API (Application programming interface) sono fondamentali per migliorare le prestazioni** degli agenti AI. Secondo il rapporto, il 60% delle aziende che utilizzano API ha migliorato la propria infrastruttura IT, mentre il 50% ha automatizzato i flussi di lavoro e il 49% ha facilitato la condivisione dei dati tra i team. Inoltre, il 51% del software interno delle aziende europee è disponibile per il riutilizzo, offrendo l'opportunità di sfruttare gli investimenti esistenti e costruire agenti AI più affidabili. Oltre a supportare gli agenti AI, le API generano un significativo valore economico. Le aziende europee che utilizzano API riportano un **aumento della produttività** (52%), una **maggiore innovazione** (47%) e una **maggiore rapidità nel soddisfare le richieste aziendali** (46%). Inoltre, i leader IT stimano che il 39% del fatturato delle loro aziende sia generato da implementazioni correlate alle API, percentuale che sale al 43% nelle organizzazioni che utilizzano agenti AI.

LE AZIENDE EUROPEE CHE UTILIZZANO API REGISTRANO UN:

aumento produttività	52%
maggiore innovazione	47%
più rapidità nel soddisfare le richieste aziendali	46%

API FONTAMENTALI PER AGENTI AI

60%

delle aziende che utilizzano API per rendere più performanti gli agenti AI, ha migliorato la propria infrastruttura IT

Verso un futuro multi-agente

Con l'aumento del numero di modelli AI utilizzati dalle aziende (passato da una media di 10 nel 2024 a 15 nel 2025), la sfida dell'integrazione diventa ancora più complessa.

Le aziende devono garantire che i diversi agenti AI possano comunicare tra loro in modo efficace, evitando duplicazioni e conflitti. Questo richiede una **strategia di integrazione proattiva che unifichi l'intero patrimonio IT**, dalle applicazioni ai sistemi, dalle automazioni alle API.

Le sfide per il futuro

Secondo **Andrew Comstock, senior vice president e general manager di MuleSoft**, *"gli agenti AI sono destinati a trasformare le aziende grazie al loro ruolo di forza lavoro digitale illimitata. Tuttavia, per sbloccare questo potenziale, l'integrazione dei dati e le API sono fondamentali per costruire una solida base per gli agenti"*. Le aziende leader devono adottare una strategia di integrazione che consenta di unificare l'intero patrimonio IT, garantendo che gli agenti AI possano **accedere a dati affidabili e operare in modo autonomo**.

L'aumento della complessità dell'infrastruttura IT rappresenta una delle principali sfide per l'adozione degli agenti AI, secondo Comstock. Con un numero crescente di applicazioni e modelli AI, le aziende rischiano di creare ulteriori silos di dati, riducendo l'efficacia degli agenti. Per affrontare questa sfida, è essenziale adottare soluzioni di integrazione che semplifichino e unifichino l'infrastruttura dei dati, consentendo agli agenti AI di operare in modo più efficiente.

Superagenti e integrazione

Il futuro degli agenti AI, secondo Comstock, sarà caratterizzato dall'emergere di **"superagenti"**, sistemi in grado di eseguire compiti complessi e multi-fase, simili a quelli umani.

Tuttavia, anche questi superagenti avranno bisogno di integrazione e automazione per funzionare in modo efficace. Le aziende dovranno investire in soluzioni di integrazione che consentano agli agenti di comunicare tra loro e di interagire con i sistemi esistenti, garantendo un **flusso di dati continuo e affidabile**.

Questa ricerca mostra il grande interesse per il mondo dell'intelligenza artificiale e, in particolare, per gli agenti, che vengono visti come una soluzione per **aumentare la produttività e l'efficienza delle aziende**, a condizione di riuscire a rendere accessibili e interconnessi tutti i dati e le applicazioni utilizzati.