Data center, in Italia ce ne sono già 153. Ecco la lista a Roma e Milano

L’Italia è un Paese per data center

La maggior parte dei **data center in Italia** si concentra nel triangolo Novara, Monza e Pavia, con **Milano** al centro. Qui se ne concentrano **un terzo del totale nazionale, che ad oggi è di 153**.

La digitalizzazione sempre più pervasiva in tutti i settori, dalle imprese alle persone, genera una quantità di dati in costante aumento. Per archiviare, elaborare e rendere disponibili questi dati è necessaria una maggiore capacità di calcolo, che si traduce in un incremento della domanda di data center.

L’accelerazione si è avuta in questi ultimi anni, per via dello sviluppo del cloud computing, dell’intelligenza artificiale (AI), del machine learning, che in particolare richiedono un’enorme potenza di calcolo, dell’internet delle cose (IoT).

In Europa (senza la **Gran Bretagna**, che ne ospita 377) il nostro Paese occupa il quarto posto per numero di data center, dopo **Germania** (406), **Francia** (244) e **Paesi Bassi** (179), secondo il Data center map.

L’aumento dei data center crea nuove opportunità di lavoro e stimola l’innovazione tecnologica, ma espongono a severi rischi, soprattutto legati alla sicurezza (la concentrazione di grandi quantità di dati in un unico luogo rende i data center un obiettivo appetibile per gli attacchi informatici),

all’approvvigionamento energetico (consumano molta energia elettrica e richiedono sistemi di raffreddamento efficienti) e alla sovranità tecnologica (è importante sviluppare un ecosistema di cloud computing nazionale per garantire l’autonomia tecnologica del paese).

Necessario un nuovo quadro regolatorio

Temi su cui in Italia si è aperto finalmente un dibattito, finalizzato alla nascita di un quadro regolatorio che tenda conti di tutti questi aspetti critici.

Per regolare questo mercato in espansione sono in corso delle audizioni ad hoc nella commissione Trasporti della Camera nell’ambio dell’esame delle proposte di legge recanti delega al Governo per la disciplina dei centri di elaborazione dati.

La cosa migliore sarebbe distribuire i datacenter su tutto il territorio nazionale (cosa che al momento non sta avvenendo). Per farlo intanto si devono garantire le stesse condizioni privilegiate legate alle autorizzazioni anche ai datacenter più piccoli. Inoltre si deve procedere a “federare” i cloud provider in modo che possano facilmente scambiarsi risorse in ambienti qualificati e certificati.

Gli investimenti in progetti più diversificati e distribuiti potrebbero avere un impatto economico più significativo e sostenibile per tutti, stimolando una crescita economica più equa e inclusiva.

Ancora meglio sarebbe costruire data center totalmente made in Italy, sia per aumentare la capacità nazionale, sia per tutelare la sovranità tecnologica, come nel caso dell’Hyper Cloud Data Center di Aruba inaugurato di recente a Roma, che va a potenziare la propria infrastruttura nazionale, rafforzando la sua presenza strategica in Italia. Un ulteriore

nodo del network di data center di proprietà del Gruppo Aruba, che comprende il Global Cloud Data Center di Ponte San Pietro (BG) e i due data center di Arezzo.

Italia hub mediterraneo?

Gli investimenti esteri in datacenter, però, non realizzano e non ampliano la sovranità digitale italiana, probabilmente semmai aumenta la dipendenza da infrastrutture estere e questo crea forte preoccupazione per chi crede nell'innovazione come drive di crescita economica. L'Europa dovrebbe aver capito che l'unico modo per crescere è sviluppare industrie locali nell'innovazione e garantire una crescita alle economie locali in un contesto competitivo.

Il nostro Paese può insomma giocare un ruolo chiave in questa partita, puntando ad esempio a divenire un hub Mediterraneo per la connettività dell'intera regione dell'Europa meridionale, per il Nord Africa e il Medio Oriente (contenendo l'influenza della Turchia e le ambizioni della Grecia).

Secondo l'ultimo Osservatorio Cloud Transformation del Politecnico di Milano, il valore investito nei data center per il 2023 è stato pari a 654 milioni, con un +10% rispetto all'anno precedente e con una potenza energetica nominale totale di 430 megawatt (+23% rispetto al 2022). L'Italia ospita circa il 12% dei 1.300 data center europei, ma ha un tasso di crescita a doppia cifra, molto superiore di Francoforte, Londra, Amsterdam, Parigi e Dublino che si attestano fra il 4% e l'8%.

Data center e AI

Diversi studi sottolineano la crescita preoccupante del consumo energetico dei data center legato allo sviluppo progressivo dell'AI. Un rapporto di *Climate Action Against Disinformation*, ad esempio, ha suggerito che l'IA potrebbe

incrementare le emissioni globali fino all’80%.

In un’altra analisi presa come riferimento in un vecchio articolo del *Wall Street Journal*, Alex de Vries, esperto di tecnologia dell’Università di Amsterdam, stima che l’IA di Google, nel peggior scenario possibile, potrebbe arrivare a consumare annualmente tanta energia quanto l’intero Stato d’Irlanda.

Secondo un report IDC si stima che la capacità dei *data center AI based* raggiungerà un tasso medio annuo di crescita del +40% fino al 2027, a cui corrisponderà un’impennata dei consumi elettrici ad un tasso medio annuo del +44,7% a 146.2 TWh entro quella data.

Complessivamente, gli studiosi si attendono un livello di consumi pari **a 857 TWh entro il 2028**, più del doppio di quelli attuali (basti pensare che il consumo energetico nazionale annuo della Gran Bretagna è stato nel 2023 pari a 266 TWh). Ovviamente, maggiori i consumi, più alte le emissioni di CO2.

Data center, la mappa italiana

In Italia come anticipato abbiamo 153 data center attivi, **50 a Milano**, 16 a Roma, 10 a Torino, 6 a Padova e diverse città con 4 (Bari, Bologna, Genova).

Più del 70% dei siti si trova nelle città del Nord (Emilia-Romagna compresa), il resto nei pressi delle principali città del Centro-Sud.



La mappa dei data center in provincia di Milano

Di seguito la lista **data center a Roma e Milano**:

A Roma:

Aruba SpA
Digital Realty
Fiber 23
C1V Hosting
IDS&Unitelm
Namex
Panservice
Unidata
Noovle S.p.A.
EXA Infrastructure
IRIDEOS
Cloud Europe S.r.l
ITnet S.r.l (IT.NET)

A Milano:

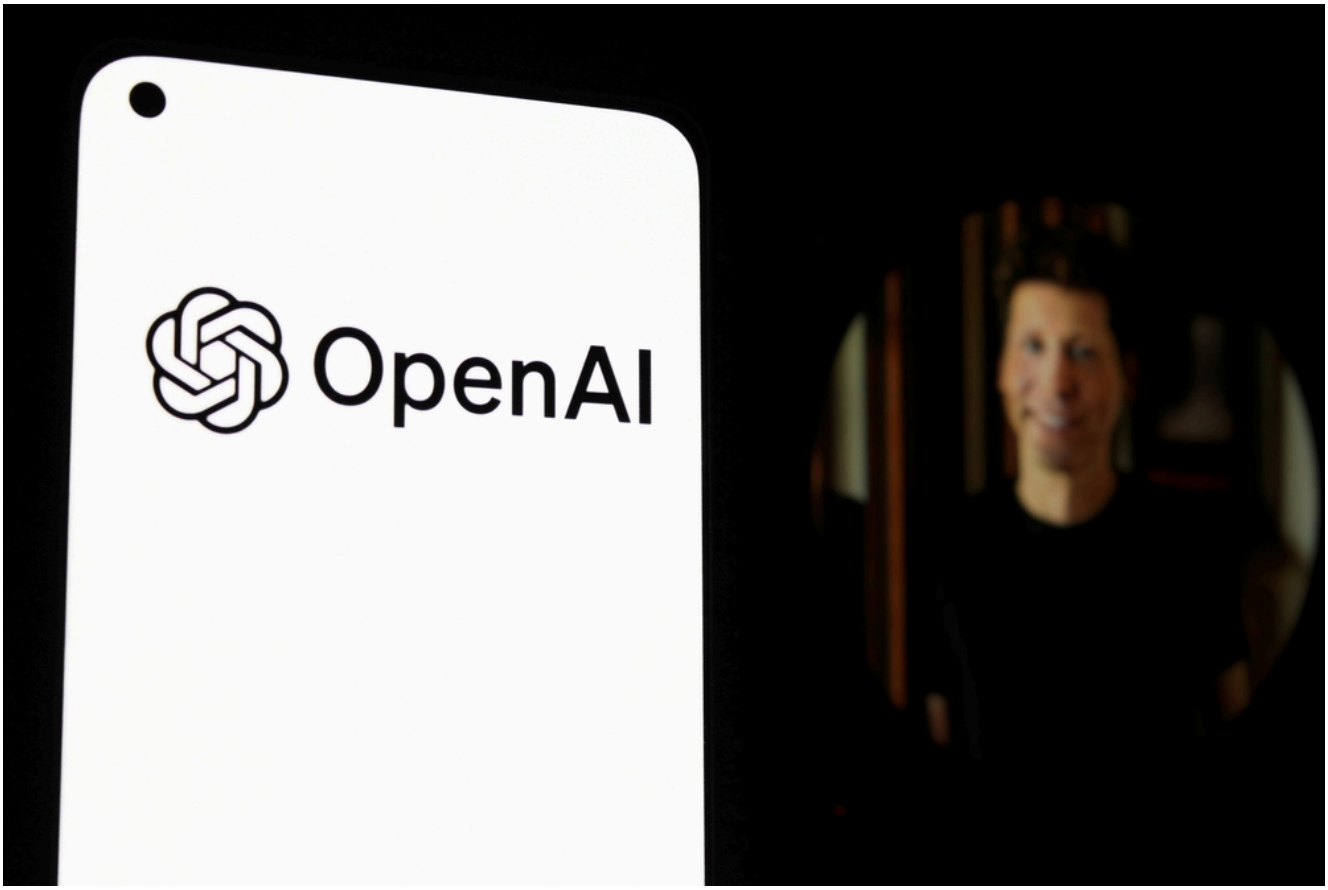
AtlasEdge
BT Services (British Telecom)
CDLAN SpA

CloudHQ
Compass Datacenters
DATA4
Elb.it
Equinix
EXA Infrastructure
FastWeb
Fiber 23
IRIDEOS
ITnet S.r.l (IT.NET)
Keppel Data Centres
Microsoft
MIX SRL
MOMIT SRL
Noovle S.p.A
Rai Way
Seeweb s.r.l.
Servereasy SRL
STACK Infrastructure
T.net Italia S.p.A.
Telnet s.r.l.
TI Sparkle
ULI
Unidata
Vantage Data Centers

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/data-center-in-italia-ce-ne-sono-gia-153-ecco-la-lista-a-roma-e-milano/515539/

OpenAI e lo strano suicidio dell’ex ricercatore Suchir Balaji. A ottobre aveva criticato l’intero settore dell’IA generativa



Suchir Balaji, ex ricercatore di **OpenAI**, è stato trovato morto nel suo appartamento di San Francisco a fine novembre, in quello che le autorità considerano un caso di suicidio. Balaji, 26 anni, aveva lasciato **OpenAI** nell’agosto 2024, citando divergenze sulle politiche aziendali, e da allora si era fatto notare per una serie di denunce pubbliche contro la società. Aveva accusato OpenAI di violare il **copyright** nel processo di addestramento dei modelli di intelligenza artificiale come **ChatGPT**, ai quali aveva lavorato per un anno e mezzo.

Balaji e l’intervista critica nei confronti di OpenAI

In un’intervista di ottobre al *New York Times*, Balaji aveva criticato l’intero settore dell’IA generativa, definendo insostenibile il modello economico basato sull’utilizzo di dati protetti da copyright senza autorizzazione. Sul suo blog, aveva spiegato che il training dei modelli generativi implica la copia di tali dati, configurando una potenziale violazione del copyright. Secondo lui, questo approccio danneggia sia le aziende che gli ecosistemi digitali, favorendo la duplicazione incontrollata di contenuti e introducendo software capaci di competere con i modelli economici tradizionali gestiti da umani.

Il suo nome è emerso in documenti legali presentati dal *New York Times* in una causa contro OpenAI, che accusa la società di aver utilizzato illegalmente materiale protetto da copyright per addestrare ChatGPT, causando danni stimati in miliardi di dollari. Balaji era indicato come uno dei detentori di informazioni cruciali per supportare queste accuse.

Nel suo account X scriveva: “Sono scettico sul fatto che il fair use possa essere una difesa plausibile per molti prodotti di AI gen”

“Ho lavorato in OpenAI per quasi 4 anni e mi sono occupato di ChatGPT nell’ultimo anno e mezzo. Inizialmente non sapevo molto su copyright, fair use, ecc., ma ho iniziato a interessarmi dopo aver visto tutte le cause legali intentate contro le aziende che sviluppano intelligenza artificiale generativa”, scriveva Suchir Balaji in un post sul suo account X. *“Cercando di comprendere meglio la questione, sono giunto*

alla conclusione che il fair use sembri una difesa piuttosto poco plausibile per molti prodotti di intelligenza artificiale generativa, principalmente perché questi possono creare sostituti che competono con i dati su cui sono addestrati. Ho scritto nel mio post i motivi più dettagliati per cui credo questo. Ovviamente, non sono un avvocato, ma penso sia comunque importante che anche i non avvocati comprendano il diritto – sia nella lettera, sia nelle ragioni per cui esiste.

"Detto ciò, non voglio che questo sembri una critica specifica a ChatGPT o a OpenAI, perché la questione del fair use e dell'intelligenza artificiale generativa è molto più ampia di un singolo prodotto o azienda. Invito vivamente i ricercatori di machine learning a informarsi di più sul diritto d'autore – è un tema davvero importante, e precedenti spesso citati, come quello di Google Books, non sono in realtà così solidi come potrebbero sembrare. Se vuoi discutere di fair use, machine learning o diritto d'autore, sentiti libero di contattarmi – penso che sia un'intersezione davvero interessante. Trovi la mia email sul mio sito personale", aveva concluso.

Elon Musk commenta con un criptico "Hmm"

Nonostante la polizia non abbia trovato prove di crimini collegati alla sua morte, la notizia ha sollevato sospetti, alimentati dal criptico commento "**Hmm**" di **Elon Musk** su X, alludendo forse a una connessione con la sua battaglia legale contro il CEO di OpenAI.

> *Hmm https://t.co/HsElym3uLV*
>
> *— Elon Musk (@elonmusk) December 14, 2024*

Musk è sempre stato critico nei confronti di OpenAI per essersi allontanata dalla sua missione originale, per il suo rapporto con Microsoft e per i potenziali rischi legati allo

sviluppo dell’IA avanzata. La sua rivalità è alimentata sia da preoccupazioni filosofiche e strategiche, sia da interessi personali e imprenditoriali nel settore dell’intelligenza artificiale. Musk ha fondato xAI nel 2023, un’azienda che si propone di sviluppare un’intelligenza artificiale alternativa in grado di competere con quella di OpenAI.

Da non-profit a profit

OpenAI è stata fondata nel 2015 come un’organizzazione no-profit con l’obiettivo di garantire che l’intelligenza artificiale beneficiasse tutta l’umanità. Ma le cose sono cambiate. A settembre la società ha annunciato che intende trasformare OpenAI in una società a scopo di lucro e Musk ha espresso preoccupazioni sul fatto che questa transizione abbia tradito gli ideali originali, mettendo il profitto sopra l’interesse collettivo.

Di recente anche Mark Zuckerberg si è schierato con Musk per bloccare la trasformazione di OpenAi in una società a scopo di lucro. Secondo il capo di Meta, consentire alla società di diventare una for-profit sarebbe un precedente pericoloso: *“Ci sarebbero significative implicazioni per la Silicon Valley. Se il nuovo modello di business di OpenAi fosse valido, gli investitori no profit otterrebbero lo stesso vantaggio chi investe in modo convenzionale in società a scopo di lucro, beneficiando anche delle detrazioni concesse dal governo”,* ha scritto Meta in una lettera di Meta al procuratore generale della California Rob Bonta.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/openai-e-lo-strano-suicidio-dellex-ricercatore-suchir-balaji-a-ottobre-aveva-criticato-lintero-settore-dellia-generativa/515500/

Internet of Offensive Things (IoOT): Cyber Crime e Infrastrutture IoT



L’evoluzione dell’Internet of Things (IoT) ha portato alla luce un fenomeno emergente nel panorama del cybercrime: l’Internet of Offensive Things (IoOT). Questo studio analizza come i dispositivi IoT vengano deliberatamente progettati o compromessi per scopi offensivi, creando una nuova categoria di minacce che sfida i paradigmi tradizionali della sicurezza informatica. La ricerca evidenzia come gli attacchi basati su IoOT stiano evolvendo da semplici botnet DDoS verso strutture più sofisticate che sfruttano l’intelligenza artificiale distribuita e l’edge computing per orchestrare attacchi multi-vettore autonomi.

Particolare attenzione viene data all’emergere di “swarm attacks”, dove dispositivi IoT compromessi collaborano in modo coordinato, adattando dinamicamente le loro strategie offensive. Lo studio presenta anche un’analisi delle contromisure emergenti, incluso l’uso di sistemi di difesa basati su blockchain e algoritmi di rilevamento anomalie zero-trust specificamente progettati per ambienti IoT ostili. Le conclusioni sottolineano l’urgente necessità di ripensare gli approcci alla sicurezza IoT in un contesto dove i dispositivi connessi possono diventare parte attiva di infrastrutture criminali autonome e auto-organizzanti.

Introduzione

L’Internet of Things ha rivoluzionato il modo in cui interagiamo con gli oggetti quotidiani, creando un ecosistema interconnesso di miliardi di dispositivi. Tuttavia, questa proliferazione di dispositivi connessi ha anche aperto nuove frontiere per le attività criminali. L’Internet of Offensive Things rappresenta un’evoluzione significativa nel panorama delle minacce cyber, dove i dispositivi IoT non sono più semplici vittime di attacchi ma diventano strumenti attivi nelle operazioni offensive.

Evoluzione delle Minacce Internet of Offensive Things (IoOT)

L’evoluzione delle minacce IoOT rappresenta uno dei più significativi cambiamenti paradigmatici nella storia del cybercrime. Partendo dalle rudimentali botnet dei primi anni 2010, abbiamo assistito a una trasformazione radicale che ha portato alla nascita di sistemi offensivi altamente sofisticati e autonomi. Il punto di svolta può essere identificato nel 2016 con l’emergere del malware Mirai, che ha dimostrato per la prima volta il potenziale devastante dei dispositivi IoT quando utilizzati come vettori di attacco coordinati.

La prima generazione di minacce IoOT si basava principalmente su tecniche di scanning indiscriminato della rete alla ricerca di dispositivi con credenziali di default o vulnerabilità note. Gli attacchi, seppur efficaci, erano relativamente semplici da un punto di vista architetturale, con strutture di comando e controllo (C2) centralizzate e un limitato set di funzionalità offensive, principalmente concentrate su attacchi DDoS.

La svolta tecnologica è avvenuta con l’introduzione di

capacità di auto-propagazione basate su tecniche di exploitation avanzate. I moderni sistemi IoOT implementano sofisticati scanner di vulnerabilità che utilizzano euristiche basate su machine learning per identificare e classificare i dispositivi target. Questi scanner sono in grado di adattare dinamicamente le loro tecniche di fingerprinting per eludere i sistemi di rilevamento, utilizzando tecniche di TCP/IP fingerprinting evasive come la frammentazione dei pacchetti e la manipolazione dei timestamp TCP.

Un aspetto particolarmente innovativo riguarda l'implementazione di sistemi di comunicazione mesh tra i dispositivi compromessi. Invece di affidarsi a server C2 centralizzati, le moderne infrastrutture IoOT utilizzano protocolli di comunicazione peer-to-peer crittografati, spesso basati su varianti modificate di protocolli esistenti come Kademlia o GNUnet. Questo approccio distribuito garantisce un'elevata resilienza dell'infrastruttura criminale, rendendo praticamente impossibile il takedown completo della rete attraverso il blocco di singoli nodi di comando.

L'integrazione di capacità di machine learning rappresenta un'altra evoluzione cruciale. I moderni sistemi IoOT implementano algoritmi di apprendimento federato che permettono ai dispositivi compromessi di condividere modelli di attacco ottimizzati senza la necessità di centralizzare i dati di training. Questo ha portato allo sviluppo di tecniche di attacco adattive che possono evolversi in risposta alle contromisure difensive implementate. Un esempio significativo è l'uso di reti neurali convoluzionali lightweight per il riconoscimento di pattern nei flussi di traffico di rete, permettendo l'identificazione automatica di obiettivi ad alto valore.

Dal punto di vista dell'architettura di sistema, le moderne infrastrutture IoOT implementano sistemi di resilienza multi-livello. Oltre ai meccanismi di comunicazione mesh, includono sistemi di backup dei dati distribuiti, capacità di migrazione

automatica delle funzionalità di comando e controllo tra i nodi, e meccanismi di auto-guarigione che possono ripristinare automaticamente le funzionalità compromesse. Particolare attenzione viene posta all'evasione dei sistemi di rilevamento, con l'implementazione di tecniche di offuscamento del traffico basate su steganografia di rete e l'uso di protocolli legitimi come covert channel.

Un aspetto particolarmente preoccupante è l'emergere di capacità di attacco multi-vettore coordinate. I moderni sistemi IoOT possono orchestrare simultaneamente diverse tipologie di attacco, dal classico DDoS all'esfiltrazione di dati, passando per attacchi di credential stuffing e cryptomining distribuito. Questa versatilità è resa possibile da un'architettura modulare che permette il caricamento dinamico di nuove funzionalità offensive, spesso distribuite attraverso reti peer-to-peer crittografate.

Le tecniche di persistenza si sono evolute ben oltre il semplice mantenimento dell'accesso al dispositivo. I moderni sistemi IoOT implementano meccanismi di sopravvivenza sofisticati che includono la modifica del firmware, l'installazione di bootkit a livello hardware, e la creazione di backdoor a livello di bootloader. Queste tecniche rendono estremamente difficile la completa rimozione dell'infezione, spesso richiedendo la sostituzione fisica dei dispositivi compromessi.

Gli attacchi basati su Internet of Offensive Things (IoOT) rappresentano una delle più sofisticate evoluzioni nel panorama delle minacce cyber contemporanee. La loro complessità tecnica si manifesta attraverso una serie di caratteristiche e metodologie operative che meritano un'analisi approfondita per comprenderne appieno il potenziale offensivo e le implicazioni per la sicurezza delle infrastrutture moderne.

La fase iniziale di un attacco IoOT tipicamente inizia con un

processo di reconnaissance avanzato che sfrutta tecniche di scanning distribuito. A differenza dei tradizionali approcci di port scanning, i dispositivi IoOT implementano metodologie di fingerprinting adattivo che utilizzano euristiche basate su machine learning per identificare e categorizzare i potenziali target. Questi scanner operano su multiple frequenze temporali, modulando dinamicamente i pattern di scanning per evitare il rilevamento. Un aspetto particolarmente innovativo è l'implementazione di tecniche di scanning cooperativo, dove multipli dispositivi coordinano le loro attività di ricognizione per costruire una mappa topologica completa della rete target senza generare pattern di traffico sospetti.

La fase di exploitation che segue la ricognizione si distingue per l'utilizzo di framework modulari di attacco che possono essere dinamicamente aggiornati attraverso canali di comunicazione peer-to-peer crittografati. Questi framework implementano sofisticate tecniche di weaponization che includono la generazione automatica di payload polimorfici, specificamente ottimizzati per le architetture hardware dei dispositivi target. Un elemento distintivo è l'utilizzo di tecniche di return-oriented programming (ROP) automatizzate che sfruttano gadget identificati dinamicamente nel firmware dei dispositivi target, permettendo l'esecuzione di codice arbitrario anche in presenza di protezioni moderne come DEP e ASLR.

L'infrastruttura di comando e controllo (C2) degli attacchi IoOT moderni implementa un'architettura ibrida che combina elementi di reti mesh con overlay networks basate su DHT (Distributed Hash Tables). La comunicazione tra i nodi utilizza protocolli proprietari che implementano tecniche di offuscamento del traffico basate su steganografia di rete avanzata. Un aspetto particolarmente sofisticato è l'implementazione di sistemi di routing anonimo ispirati a Tor ma ottimizzati per le limitazioni hardware dei dispositivi IoT, che permettono di mascherare efficacemente l'origine e la

destinazione del traffico di comando.

La persistenza negli attacchi IoOT viene garantita attraverso tecniche di rootkitting a più livelli che modificano il firmware dei dispositivi compromessi. Queste modifiche vengono effettuate utilizzando tecniche di code injection che sfruttano vulnerabilità nelle routine di aggiornamento del firmware per installare backdoor persistenti. Un aspetto innovativo è l'implementazione di meccanismi di "firmware camouflage" che permettono al codice malevolo di sopravvivere anche ai tentativi di ripristino del firmware originale, attraverso la modifica delle partizioni di recovery.

La capacità offensiva degli attacchi IoOT è ulteriormente potenziata dall'implementazione di sistemi di attacco multi-stage che operano su diverse temporalità. La prima fase tipicamente prevede la creazione di una rete dormiente di dispositivi compromessi che rimangono in attesa utilizzando tecniche di comunicazione stealth basate su timing channels e covert channels costruiti su protocolli legittimi. Questi dispositivi possono essere attivati in modo coordinato attraverso trigger complessi che includono condizioni temporali, eventi di rete specifici o pattern di traffico predefiniti.

Un aspetto particolarmente avanzato riguarda l'implementazione di capacità di lateral movement che sfruttano tecniche di pivoting automatizzato. I dispositivi compromessi implementano scanner di vulnerabilità integrati che possono identificare e sfruttare automaticamente vulnerabilità zero-day attraverso l'uso di fuzzing distribuito e tecniche di exploit generation basate su machine learning. Questi sistemi sono in grado di adattare dinamicamente le loro strategie di exploitation basandosi sul feedback raccolto da tentativi precedenti, implementando una forma di "apprendimento offensivo" distribuito.

La fase di attacco attivo si distingue per l'implementazione

di tecniche di resource amplification avanzate che permettono di massimizzare l'impatto offensivo anche con dispositivi dalle risorse limitate. Questo include l'uso di tecniche di reflection e amplification DDoS ottimizzate, combinate con attacchi di protocol abuse che sfruttano vulnerabilità intrinseche nei protocolli di rete standard. Un elemento distintivo è l'implementazione di tecniche di "protocol mutation" che permettono di generare varianti di attacchi noti per eludere i sistemi di rilevamento basati su signature.

L'esfiltrazione dei dati negli attacchi IoOT moderni utilizza tecniche di data tunneling multiprotocollo che nascondono il traffico malevolo all'interno di stream di dati apparentemente legittimi. Questo include l'uso di tecniche di stenografia di rete avanzata che sfruttano campi poco utilizzati nei protocolli standard come vettori per il trasporto di dati esfiltrati. La robustezza di questi canali viene garantita attraverso l'implementazione di sistemi di error correction distribuiti che possono ricostruire i dati anche in presenza di significativa perdita di pacchetti.

Swarm Intelligence negli Attacchi IoOT

La **Swarm Intelligence** (SI), o **intelligenza a sciame**, è un campo dell'**intelligenza artificiale** che si ispira al comportamento collettivo di gruppi di organismi naturali, come sciami di api, stormi di uccelli, colonie di formiche o banchi di pesci. Questi sistemi biologici mostrano capacità emergenti di risolvere problemi complessi attraverso il coordinamento di individui relativamente semplici e decentralizzati. La Swarm Intelligence rappresenta un approccio bio-ispirato estremamente utile per risolvere problemi complessi in ambienti dinamici, con grande applicabilità nelle tecnologie emergenti e nei sistemi distribuiti che però ha visto l'utilizzo anche in ambito cyber crime.

Il concetto di Swarm Intelligence, originariamente ispirato dal comportamento degli insetti sociali, ha trovato una sua inquietante applicazione nel contesto degli attacchi IoOT, dando vita a una nuova generazione di minacce particolarmente insidiose. L'implementazione di questi principi nel cybercrime ha portato allo sviluppo di infrastrutture offensive che mostrano caratteristiche emergenti di intelligenza collettiva, dove il comportamento coordinato dell'insieme supera significativamente le capacità dei singoli dispositivi compromessi.

Nel contesto degli attacchi IoOT, l'architettura swarm si basa su un sistema di comunicazione distribuito che implementa algoritmi di consenso modificati, derivati da protocolli blockchain ma ottimizzati per operazioni in tempo reale. Ogni dispositivo compromesso opera come un nodo autonomo all'interno dello sciame, mantenendo una visione parziale dello stato globale dell'attacco attraverso un sistema di gossip protocol crittografato. Questo approccio garantisce che nessun nodo singolo possieda informazioni complete sull'infrastruttura, rendendo estremamente difficile la comprensione della topologia dell'attacco anche quando alcuni dispositivi vengono compromessi dai difensori.

L'aspetto più innovativo di questi sistemi risiede nei meccanismi di auto-organizzazione basati su algoritmi di ottimizzazione distribuita. Gli sciami IoOT implementano varianti modificate dell'algoritmo Particle Swarm Optimization (PSO), adattate per operare in contesti di rete distribuiti. Ogni dispositivo compromesso mantiene e aggiorna continuamente un set di parametri di attacco, condividendo i risultati delle proprie azioni con i nodi vicini attraverso un sistema di feedback ponderato. Questo processo permette allo sciame di identificare e replicare automaticamente le strategie di attacco più efficaci, adattandosi dinamicamente alle contromisure difensive implementate.

La resilienza di questi sistemi è garantita da un sofisticato

meccanismo di auto-guarigione basato su tecniche di quorum sensing distribuite. Quando parti dello sciame vengono compromesse o isolate, i nodi rimanenti sono in grado di riorganizzarsi autonomamente, ribilanciando il carico di attacco e modificando la topologia della rete per mantenere l'efficacia operativa. Questo comportamento emergente si manifesta attraverso l'implementazione di algoritmi di consenso probabilistici che permettono decisioni coordinate anche in presenza di significativa perdita di nodi.

Un elemento particolarmente preoccupante è l'implementazione di capacità di apprendimento collettivo. Gli sciami IoOT moderni utilizzano tecniche di federated learning modificate per condividere e aggregare le informazioni sulle vulnerabilità scoperte e sull'efficacia delle diverse tecniche di attacco. Ogni dispositivo mantiene un modello locale leggero basato su reti neurali ricorrenti (RNN) che viene periodicamente aggiornato attraverso un processo di aggregazione distribuita. Questo permette allo sciame di sviluppare e perfezionare continuamente nuove tecniche di attacco, adattandosi in tempo reale alle difese incontrate.

La coordinazione tattica degli attacchi viene gestita attraverso un sistema di stigmergia digitale, dove i dispositivi compromessi lasciano "tracce" crittografate nel traffico di rete che influenzano il comportamento degli altri membri dello sciame. Questo approccio, ispirato ai sistemi di comunicazione delle colonie di formiche, permette una coordinazione efficace senza richiedere una comunicazione diretta tra i nodi, rendendo estremamente difficile l'identificazione e il blocco dei canali di comando e controllo.

L'efficacia di questi sistemi è ulteriormente potenziata dall'implementazione di meccanismi di specializzazione dinamica dei ruoli. All'interno dello sciame, i dispositivi possono assumere ruoli diversi basati sulle loro capacità hardware e sulla loro posizione nella rete. Alcuni nodi

possono specializzarsi nella ricognizione, utilizzando tecniche di network scanning evasive basate su algoritmi genetici per l'ottimizzazione dei pattern di scanning. Altri possono focalizzarsi sull'exploitation, implementando sistemi esperti distribuiti per la selezione e l'esecuzione degli exploit più appropriati per ogni target identificato.

La natura distribuita e auto-organizzante di questi attacchi pone sfide significative per i sistemi di difesa tradizionali. L'assenza di un punto di comando centralizzato, combinata con la capacità dello sciame di adattarsi e evolversi autonomamente, rende estremamente difficile l'implementazione di contromisure efficaci. Inoltre, la capacità degli sciami di operare con successo anche in presenza di elevata latenza e connettività intermittente li rende particolarmente adatti per attacchi su larga scala che coinvolgono dispositivi IoT con risorse limitate.

Contromisure e Strategie Difensive

La difesa contro le minacce IoOT richiede un approccio multidimensionale che va ben oltre le tradizionali misure di sicurezza perimetrale. L'evoluzione delle capacità offensive ha reso necessario lo sviluppo di sistemi di protezione che operano su multiple dimensioni temporali e spaziali, implementando meccanismi di difesa adattiva capaci di contrastare la natura distribuita e autonoma degli attacchi moderni.

Nel cuore delle moderne strategie difensive troviamo implementazioni avanzate di sistemi zero-trust specificamente progettati per ambienti IoT. Questi sistemi si basano su un'architettura di microsegmentazione dinamica che utilizza tecniche di Software Defined Networking (SDN) per creare e gestire domini di sicurezza isolati. La particolarità di questi sistemi risiede nell'implementazione di politiche di accesso context-aware che vengono continuamente ricalcolate

basandosi su multipli fattori di rischio, inclusi pattern comportamentali, anomalie nelle comunicazioni e indicatori di compromissione distribuiti.

L'autenticazione dei dispositivi IoT viene gestita attraverso sistemi di Identity and Access Management (IAM) distribuiti che implementano protocolli di mutual authentication basati su crittografia a curve ellittiche (ECC). Un aspetto innovativo è l'utilizzo di tecniche di device fingerprinting comportamentale che creano profili di autenticazione multi-dimensionali basati non solo sulle caratteristiche hardware del dispositivo, ma anche sui suoi pattern di comunicazione e utilizzo delle risorse. Questi profili vengono continuamente aggiornati attraverso tecniche di machine learning non supervisionato che possono identificare deviazioni sottili dal comportamento atteso.

La detection delle minacce si basa su sistemi di Network Behavior Analysis (NBA) che implementano algoritmi di anomaly detection distribuiti. Questi sistemi utilizzano reti neurali ricorrenti (RNN) ottimizzate per operare su stream di dati ad alta velocità, capaci di identificare pattern di attacco complessi anche quando distribuiti su multiple dimensioni temporali. Un elemento distintivo è l'implementazione di tecniche di correlation analysis che possono aggregare eventi apparentemente non correlati per identificare campagne di attacco coordinate.

Un aspetto cruciale della difesa riguarda l'implementazione di sistemi di deception technology specificamente progettati per ambienti IoT. Questi sistemi creano honeypot dinamici che emulano dispositivi IoT vulnerabili, implementando stack di protocollo completi e comportamenti realistici. La particolarità di questi sistemi reside nella loro capacità di adattarsi dinamicamente agli attacchi, modificando la propria superficie di attacco per massimizzare l'engagement con gli attaccanti e raccogliere intelligence sulle loro tecniche operative.

La risposta agli incidenti viene gestita attraverso sistemi di Automated Response and Remediation (ARR) che possono implementare contromisure in tempo reale. Questi sistemi utilizzano tecniche di orchestrazione security basate su playbook dinamici che vengono continuamente ottimizzati attraverso tecniche di reinforcement learning. Un elemento innovativo è l'implementazione di meccanismi di "surgical containment" che possono isolare selettivamente parti compromesse della rete mantenendo operative le funzionalità critiche.

La resilienza dell'infrastruttura viene garantita attraverso l'implementazione di sistemi di "security mesh" distribuiti che creano overlay networks di sicurezza dinamiche. Questi sistemi implementano meccanismi di fail-over automatico e load balancing dei controlli di sicurezza, permettendo di mantenere un livello di protezione elevato anche in presenza di compromissioni parziali dell'infrastruttura. Un aspetto particolare è l'utilizzo di tecniche di "security state synchronization" che permettono di mantenere una visione coerente dello stato di sicurezza attraverso l'intera infrastruttura distribuita.

Il monitoraggio continuo dell'infrastruttura viene realizzato attraverso sistemi di Security Information and Event Management (SIEM) distribuiti che implementano capacità di analisi in tempo reale basate su stream processing. Questi sistemi utilizzano tecniche di complex event processing per identificare sequenze di eventi che potrebbero indicare attacchi in corso, implementando capacità di predictive analytics basate su modelli di machine learning che possono anticipare possibili vettori di attacco.

La gestione delle vulnerabilità in ambienti IoT richiede approcci innovativi che vanno oltre il tradizionale vulnerability scanning. I moderni sistemi implementano tecniche di "continuous security posture assessment" che combinano vulnerability scanning attivo con passive monitoring

e configuration analysis. Un elemento distintivo è l'implementazione di sistemi di "risk-based prioritization" che utilizzano algoritmi di graph analysis per identificare i dispositivi e le vulnerabilità che rappresentano il maggior rischio per l'infrastruttura complessiva.

La protezione del firmware dei dispositivi IoT viene realizzata attraverso sistemi di "secure boot" e "runtime integrity monitoring" che implementano meccanismi di attestazione remota basati su hardware security modules (HSM). Questi sistemi possono verificare continuamente l'integrità del firmware e del software in esecuzione, identificando e bloccando tentativi di modifica non autorizzata. Un aspetto innovativo è l'implementazione di tecniche di "firmware diversity" che creano varianti uniche del firmware per ogni dispositivo, rendendo più difficile lo sviluppo di exploit generalizzati.

Sfide Future e Direzioni di Ricerca

L'evoluzione dell'Internet of Offensive Things presenta una serie di sfide tecniche e di ricerca che richiederanno innovazioni significative nel campo della sicurezza informatica nei prossimi anni. La crescente sofisticazione degli attacchi IoOT, combinata con l'espansione continua dell'ecosistema IoT, sta creando nuovi scenari di minaccia che necessitano di approcci rivoluzionari per essere affrontati efficacemente.

Una delle sfide più pressanti riguarda lo sviluppo di sistemi di detection capaci di identificare attacchi distribuiti complessi che operano su scale temporali estese. I tradizionali approcci basati su signature detection o anomaly detection si stanno dimostrando insufficienti di fronte a attacchi che utilizzano tecniche di evasione avanzate e comportamenti mimetici. La ricerca si sta orientando verso lo sviluppo di sistemi di detection che implementano architetture

neurali profonde specializzate nell'analisi di serie temporali multidimensionali.

Questi sistemi dovranno essere capaci di operare in tempo reale su stream di dati ad alta velocità, mantenendo al contempo la capacità di identificare pattern di attacco che si sviluppano su periodi estesi di tempo. Un aspetto particolarmente promettente riguarda l'utilizzo di tecniche di attention mechanism personalizzate per l'analisi del traffico IoT, capaci di focalizzare l'analisi su sequenze di eventi potenzialmente malevoli anche in presenza di grandi volumi di traffico legittimo.

Il problema della scalabilità delle difese rappresenta un'altra sfida cruciale. Con la proliferazione dei dispositivi IoT, i sistemi di sicurezza devono essere in grado di gestire milioni di endpoint mantenendo capacità di risposta in tempo reale. La ricerca sta esplorando architetture di sicurezza distribuite che implementano tecniche di edge computing avanzato, dove le capacità di analisi e risposta vengono distribuite su multiple layer di processamento. Un approccio innovativo riguarda lo sviluppo di sistemi di "federated security" che permettono la collaborazione tra domini di sicurezza indipendenti mantenendo la privacy e l'isolamento dei dati sensibili. Questi sistemi dovranno implementare meccanismi di consensus distribuito ottimizzati per ambienti IoT, capaci di raggiungere decisioni coordinate anche in presenza di latenza elevata e connettività intermittente.

L'autenticazione sicura in ambienti IoT ad alta dinamicità rappresenta una sfida tecnica particolarmente complessa. I tradizionali approcci basati su PKI centralizzate si stanno dimostrando inadeguati per scenari dove i dispositivi entrano ed escono continuamente dalla rete e dove le relazioni di trust devono essere stabilite dinamicamente. La ricerca sta esplorando sistemi di autenticazione basati su blockchain che implementano meccanismi di "dynamic trust establishment" attraverso smart contract specializzati. Un aspetto innovativo

riguarda lo sviluppo di protocolli di autenticazione lightweight che possono operare efficacemente anche su dispositivi con risorse limitate, utilizzando tecniche di crittografia post-quantum per garantire la sicurezza a lungo termine.

La gestione dell'identità e dell'accesso in ecosistemi IoT complessi richiede nuovi paradigmi che vadano oltre i tradizionali modelli RBAC (Role-Based Access Control). La ricerca si sta orientando verso lo sviluppo di sistemi ABAC (Attribute-Based Access Control) distribuiti che possono valutare multipli attributi contestuali in tempo reale per prendere decisioni di accesso granulari. Un aspetto particolarmente sfidante riguarda l'implementazione di meccanismi di "continuous authentication" che possono verificare continuamente l'identità e l'integrità dei dispositivi durante l'intera durata della loro operatività, utilizzando tecniche di behavioral biometrics adattate per il contesto IoT.

Il bilanciamento tra sicurezza e performance rappresenta una sfida persistente che richiede approcci innovativi. La ricerca sta esplorando tecniche di "adaptive security" che possono modulare dinamicamente il livello di protezione basandosi sul contesto operativo e sul livello di rischio percepito. Un elemento promettente riguarda lo sviluppo di algoritmi di ottimizzazione multi-obiettivo che possono bilanciare automaticamente requisiti contrastanti di sicurezza, performance e consumo energetico. Questi sistemi dovranno implementare meccanismi di "security-aware scheduling" che possono allocare risorse di sicurezza in modo ottimale attraverso l'infrastruttura distribuita.

La protezione contro attacchi quantum rappresenta una sfida emergente che richiederà innovazioni significative nei prossimi anni. Con l'avvento dei computer quantistici, molti degli attuali meccanismi crittografici utilizzati negli ambienti IoT diventeranno vulnerabili. La ricerca sta

esplorando l'implementazione di algoritmi crittografici post-quantum ottimizzati per dispositivi IoT, un compito particolarmente sfidante considerando i limiti di risorse di questi dispositivi. Un approccio promettente riguarda lo sviluppo di sistemi ibridi che combinano crittografia classica e quantum-resistant, permettendo una transizione graduale verso architetture completamente quantum-safe.

L'analisi forense in ambienti IoT distribuiti presenta sfide uniche che richiedono nuovi approcci metodologici e tecnici. La ricerca sta esplorando tecniche di "distributed forensics" che possono raccogliere e correlare evidenze da multipli dispositivi IoT mantenendo la catena di custodia digitale. Un aspetto innovativo riguarda lo sviluppo di sistemi di "predictive forensics" che possono anticipare e preservare evidenze potenzialmente rilevanti prima che vengano compromesse o perse. Questi sistemi dovranno implementare meccanismi di "forensic-ready logging" distribuiti che possono registrare eventi rilevanti in modo sicuro e verificabile.

Le considerazioni etiche e legali nell'ambito della sicurezza IoT rappresentano una sfida multidimensionale che richiede un approccio interdisciplinare. La ricerca sta esplorando framework etici specifici per l'IoT che possono guidare lo sviluppo di sistemi di sicurezza rispettosi della privacy e dei diritti individuali. Un aspetto particolarmente sfidante riguarda lo sviluppo di meccanismi di "privacy-preserving security" che possono garantire elevati livelli di protezione mantenendo al contempo la confidenzialità dei dati personali. Questi sistemi dovranno implementare tecniche di "privacy by design" che integrano considerazioni sulla privacy fin dalle prime fasi della progettazione dei sistemi di sicurezza.

Conclusioni

L'Internet of Offensive Things rappresenta una sfida significativa per la sicurezza informatica moderna. La

crescente sofisticazione degli attacchi, combinata con l'emergere di comportamenti di tipo swarm, richiede un ripensamento fondamentale degli approcci alla sicurezza IoT. È essenziale sviluppare strategie difensive che possano anticipare e contrastare queste minacce emergenti, considerando sia gli aspetti tecnici che quelli etici e legali.

Fonti:

- "A quorum sensing pattern for multi-agent self-organizing security systems" Jeff Hamar e Rick Dove (2012);
- "Swarm Intelligence-Based Algorithms within IoT-Based Systems: a Review" Ouarda Zedadra, Antonio Guerrieri, Nicolas Jouandeau, Giandomenico Spezzano, Hamid Seridi, Giancarlo Fortino (2018);
- "A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges" Tinshu Sasi, Arash Habibi Lashkari, Rongxing Lu, Pulei Xiong (2023) "A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges";
- "A Blockchain-based approach for secure IoT" Sonia Kotel, Fatma Sbiaa, Raouda Maraoui Kamoun, Lazhar Hamel (2023);
- "Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures" Claudio Zanasi, Silvio Russo, Michele Colajanni (2024);
- "The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws" Ashwin Karale (2021).

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/internet-of-offensive-things/

Klarna ha interrotto da un anno tutte le assunzioni per sostituire i lavoratori con l’AI



Klarna, la nota azienda di pagamenti digitali, ha deciso un anno fa di interrompere completamente le assunzioni per avviare un piano strategico volto alla sostituzione di alcune figure lavorative con sistemi di AI.

Questa scelta rappresenta un passaggio significativo nell’adozione di tecnologie automatizzate per migliorare l’efficienza e ridurre i costi operativi, pur sollevando questioni etiche e sociali. L’azienda ha progressivamente integrato l’AI in diversi settori, come il servizio clienti, la gestione dei dati e i processi di analisi del rischio.

I dirigenti di Klarna sostengono che l’uso di sistemi

automatizzati abbia aumentato la produttività e permesso di offrire soluzioni più rapide e personalizzate agli utenti. Tuttavia, la decisione di non ampliare il personale umano ha generato critiche, soprattutto riguardo alle implicazioni per l'occupazione e l'impatto sul mercato del lavoro.

Secondo fonti interne, questa mossa rientra in una strategia a lungo termine per consolidare la posizione dell'azienda in un settore sempre più competitivo, dove l'AI viene considerata una leva essenziale per innovare e rimanere al passo con le aspettative dei consumatori.

Nonostante i benefici economici, molti esperti sottolineano i rischi legati all'eccessiva dipendenza dalla tecnologia, come possibili errori nei processi decisionali automatizzati e una riduzione della supervisione umana.

La scelta di Klarna evidenzia un trend crescente in cui le aziende tecnologiche investono nelle potenzialità dell'intelligenza artificiale per ottimizzare i propri servizi. Tuttavia, il caso solleva domande importanti sul bilanciamento tra innovazione, responsabilità sociale e impatti occupazionali.

Per maggiori informazioni, clicca per **l'articolo originale**.

Il Messico utilizza un'app basata su AI per ridurre i suicidi nello Yucatán

Nello stato messicano dello Yucatán, l'app MeMind, supportata da tecnologie AI, ha permesso di identificare e trattare oltre 10.000 persone a rischio di suicidio, contribuendo a una riduzione del 9% del tasso di suicidi. L'iniziativa è nata dalla necessità di affrontare un problema endemico: lo Yucatán registra infatti un tasso di suicidi doppio rispetto al resto del Paese.

Attraverso questionari dettagliati e un algoritmo che analizza i comportamenti degli utenti, l'app individua segnali di rischio e fornisce supporto, come check-in personalizzati e indicazioni verso terapie o gruppi di aiuto. L'app, utilizzata da circa 80.000 persone, rappresenta una risposta innovativa alla crescente crisi globale di salute mentale, specialmente tra i giovani.

Tuttavia, non mancano le sfide: la copertura tecnologica è limitata in alcune aree e il gruppo più vulnerabile, i giovani uomini, è anche il meno propenso a usare regolarmente l'app.

I dati raccolti dall'app sono utilizzati anche per orientare le politiche pubbliche in materia di salute mentale. Critiche emergono sul fatto che l'app affronti solo i sintomi di problemi più profondi, come stagnazione economica e disuguaglianze sociali.

Nonostante ciò, il progetto è considerato un esempio positivo di come l'AI possa migliorare l'accessibilità alle cure e abbattere stigmi sociali. I piani futuri includono l'integrazione di chatbot per rendere le interazioni più empatiche e ridurre il senso di giudizio spesso percepito nei confronti dei terapeuti umani.

Per maggiori informazioni, clicca per **l'articolo originale**.

Gli Stati Uniti si preparano a nuove restrizioni sui chip AI per chiudere l'accesso indiretto della Cina

Gli Stati Uniti stanno pianificando di intensificare le restrizioni sull'esportazione di chip avanzati per AI, con l'obiettivo di impedire alla Cina di accedere a queste tecnologie cruciali attraverso canali alternativi. Le nuove

norme intendono bloccare ogni forma di collaborazione o utilizzo indiretto, eliminando così potenziali ‘scappatoie’.

Questo intervento si colloca in un contesto di crescente tensione geopolitica, in cui l’innovazione tecnologica rappresenta una leva strategica per il dominio globale. Questi chip, fondamentali per lo sviluppo di sistemi di intelligenza artificiale avanzata, rappresentano una risorsa chiave per la supremazia tecnologica. Il governo statunitense teme che Pechino possa sfruttare queste tecnologie per rafforzare il proprio settore militare e incrementare il controllo interno, compromettendo così la sicurezza globale.

Inoltre, l’accesso della Cina ai chip tramite Paesi terzi o partnership commerciali rappresenta una preoccupazione centrale che le nuove regolamentazioni mirano a eliminare. Il Dipartimento del Commercio degli Stati Uniti sta quindi progettando regole più severe, includendo restrizioni su alleanze strategiche e vendite transnazionali.

Le misure riflettono la crescente rivalità tecnologica tra le due maggiori economie mondiali, ma sollevano anche interrogativi sull’impatto per l’industria globale dei semiconduttori. Alcune aziende tecnologiche statunitensi temono che restrizioni più rigide possano limitare la loro capacità di competere sui mercati internazionali.

Questo intervento dimostra l’urgenza percepita dagli Stati Uniti nel mantenere un vantaggio competitivo nell’ecosistema AI, riducendo il rischio che tecnologie critiche possano essere utilizzate da governi ostili per scopi non conformi agli interessi occidentali.

Per maggiori informazioni, clicca per **l’articolo originale**.

Madonna alimenta lo scontro

decennale con la Chiesa con immagini AI del Papa

Madonna ha suscitato polemiche condividendo sui social immagini generate con AI che la ritraggono in pose ambigue con Papa Francesco. Le foto, manipolate digitalmente, mostrano la cantante e il pontefice in atteggiamenti intimi, scatenando critiche sulla mancanza di etica nell'uso dell'AI e del digitale.

Le reazioni sono state polarizzate: alcuni utenti le hanno definite irrispettose e inappropriate, mentre altri le hanno percepite come una provocazione ironica.

La relazione complessa tra Madonna e la Chiesa cattolica non è nuova. La popstar, cresciuta in una famiglia cattolica, è stata spesso al centro di controversie per il suo uso di simboli religiosi, dalla canzone 'Like a Virgin' fino alla pubblicazione del libro *Sex*.

La Chiesa, in passato, ha pubblicamente condannato le sue performance, arrivando a chiedere il boicottaggio di concerti come il *Blond Ambition Tour*. Tuttavia, Madonna ha spesso integrato elementi spirituali nei suoi lavori, descrivendo la propria fede come un mix di tradizioni religiose diverse.

Le recenti immagini hanno riacceso il dibattito sull'etica dell'AI e sull'uso responsabile delle tecnologie digitali. Critici e sostenitori si interrogano sul confine tra libertà artistica e rispetto per la religione, mentre emergono domande più ampie sulla regolamentazione dell'AI per evitare usi potenzialmente dannosi o offensivi.

Per maggiori informazioni, clicca per **l'articolo originale**.

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/klarna-ha-interrotto-da-un-anno-tutte-l

e-assunzioni-per-sostituire-i-lavoratori-con-lai/515486/

Cybersecurity in Italia: sfide e opportunità secondo l'Agenzia per la Cybersicurezza Nazionale (ACN)

Nell'intervento di apertura del 22° Forum ICT Security, Luca Nicoletti – Capo del Servizio Programmi Industriali, Tecnologici e di Ricerca dell'Agenzia per la Cybersicurezza Nazionale (ACN) – ha offerto un'analisi complessiva delle sfide e delle opportunità nel settore della cybersecurity in Italia.

"Come paese e come continente, non possiamo più rimandare la spinta verso l'innovazione" ha dichiarato Nicoletti, enfatizzando l'urgenza di un approccio strutturato e coordinato alla cybersicurezza.

Il suo discorso è stato un richiamo all'azione: richiamando le prime edizioni del Forum e i profondi cambiamenti verificatisi da allora, il rappresentante dell'Agenzia ha evidenziato la necessità di definire risposte condivise tra tutti gli attori coinvolti, sia pubblici che privati.

Cybersecurity in Italia:

Trasformazione Digitale e superficie di attacco

Negli ultimi anni la trasformazione digitale ha radicalmente ridefinito il panorama della cybersecurity in Italia.

La crescente interconnessione dei dispositivi e delle reti ha ampliato la superficie di attacco fino a coinvolgere ogni aspetto della vita quotidiana, dall'IoT domestico alle infrastrutture critiche nazionali: questa espansione richiede un approccio olistico alla sicurezza, che tenga conto anche delle molteplici dipendenze tra i vari sistemi.

Di conseguenza, ciò che vent'anni fa poteva sembrare frutto di una visione futuristica è oggi un pilastro essenziale per garantire la continuità del sistema produttivo e la protezione dei dati personali all'interno di ecosistemi sempre più interconnessi.

In questo contesto, la cybersicurezza è divenuta un elemento imprescindibile per aziende e organizzazioni; la crescita esponenziale della connettività e la crescente adozione di tecnologie avanzate comportano infatti un aumento significativo delle vulnerabilità, rendendo la protezione di sistemi e informazioni una priorità assoluta per qualsiasi Stato.

Evoluzione del quadro normativo europeo

Il quadro normativo europeo è in continua evoluzione per rispondere adeguatamente a queste sfide. Il *Cyber Solidarity Act* rappresenta una pietra miliare nell'ambito della cooperazione transnazionale, introducendo elementi cruciali come i *Rapid Reaction Teams* (RRT).

Nicoletti ha descritto gli RRT come *"unità di reazione rapida*

che saranno capaci di supportare tutti noi nel ripartire da incidenti”: integrando competenze in ambito di *threat hunting, digital forensics* e *incident response*, questi team rappresentano un significativo passo avanti nella gestione delle crisi informatiche.

Inoltre, il framework normativo introduce protocolli standardizzati per la condivisione delle informazioni sulle minacce e meccanismi di coordinamento internazionale per la gestione degli incidenti; la capacità di strategie concertate tra i vari Stati membri dell’Unione è fondamentale per garantire una difesa comune che sappia rispondere con efficacia agli attacchi informatici, sempre più spesso caratterizzati da una portata globale.

La Direttiva NIS2 – entrata in vigore il 16 ottobre – costituisce un altro pilastro fondamentale della strategia di sicurezza dell’Unione Europea. La NIS2 stabilisce infatti requisiti tecnici rigorosi per la *security by design*, standard di *reporting* degli incidenti e parametri di resilienza informatica: l’obiettivo è migliorare la sicurezza di sistemi e servizi digitali, promuovendo una gestione proattiva del rischio e una maggiore trasparenza nei processi.

In ossequio alla direttiva, le organizzazioni dovranno implementare misure di sicurezza più stringenti, mostrandosi capaci di rispondere alle minacce informatiche in continua evoluzione.

Questa regolamentazione è essenziale per creare ecosistemi sicuri e resilienti, in grado di sostenere la trasformazione digitale senza comprometterne la sicurezza.

Infrastrutture Strategiche e calcolo ad alte prestazioni

Un progetto strategico su cui l’ACN sta concentrando grandi

sforzi è lo sviluppo di un'infrastruttura di calcolo ad alte prestazioni (HPC) a Napoli.

"Con i fondi PNRR stiamo realizzando un importante calcolatore di high-performance computing", ha spiegato Nicoletti; la piattaforma sarà utilizzata per il *machine learning*, l'analisi predittiva delle minacce e la ricerca in campo di crittografia quantistica e post-quantistica.

L'infrastruttura HPC non solo rafforzerà la capacità tecnologica del paese ma fungerà anche da catalizzatore per la ricerca e l'innovazione, al fine di rendere disponibile una risorsa di calcolo avanzata utilizzabile dall'ACN per rafforzare la sicurezza nazionale, nonché dal mondo accademico e industriale per sviluppare soluzioni all'avanguardia.

Questo progetto rappresenta un esempio concreto di come i fondi pubblici possano essere sfruttati per potenziare le infrastrutture strategiche e supportare la crescita del paese, favorendo lo sviluppo di competenze e la creazione di valore aggiunto in ambito tecnologico e scientifico.

Sfide tecnologiche emergenti: IA e Quantum Computing

Le sfide tecnologiche emergenti, in particolare l'Intelligenza Artificiale e il *computing* quantistico, richiedono una particolare attenzione.

L'Intelligenza Artificiale – ha sottolineato Nicoletti – *"è entrata prepotentemente nella nostra vita quotidiana e, come tutte le nuove tecnologie, rappresenta al tempo stesso un'opportunità e un rischio*".

Se infatti l'uso dell'IA nella cybersicurezza rappresenta una frontiera dalle enormi potenzialità, deve essere gestito con grande attenzione per evitare rischi associati all'abuso di

queste tecnologie e alle loro possibili implicazioni etiche.

L'ACN sta già lavorando all'implementazione di sistemi di *threat detection* basati sull'IA e allo sviluppo di algoritmi di analisi comportamentale per migliorare la sicurezza nazionale; qesti sistemi consentono di rilevare anomalie nei flussi di dati in modo più rapido ed efficiente, rendendo possibile una risposta tempestiva alle minacce.

Parallelamente, anche il *computing* quantistico rappresenta una sfida senza precedenti.

"Gli algoritmi di crittografia che utilizziamo quotidianamente" ha avvertito Nicoletti *"e tra pochi anni probabilmente saranno obsoleti".*

Il *computing* quantistico ha quindi il potenziale di compromettere gli attuali metodi crittografici, rendendo vulnerabili i dati sensibili: uno scenario che impone un'urgente transizione verso algoritmi *quantum-resistant* e una revisione completa dei protocolli di sicurezza esistenti, al fine di sviluppare nuovi sistemi di crittografia resistenti ai futuri attacchi quantistici.

La ricerca su questi temi è già in corso, ma richiede investimenti sostanziali e un impegno strategico per garantire che le tecnologie siano pronte prima che il *computing* quantistico diventi una minaccia concreta per la sicurezza informatica.

Investimenti e programmi di sviluppo

Sul fronte dei finanziamenti, l'ACN ha già impegnato **600 milioni di euro dai fondi del Piano Nazionale di Ripresa e Resilienza (PNRR) per lo sviluppo di infrastrutture critiche e il potenziamento delle capacità di *monitoring***.

Questi investimenti sono destinati sia a rafforzare le infrastrutture esistenti, sia a sviluppare nuove soluzioni per migliorare la resilienza e la sicurezza del paese; sebbene una parte significativa sia vincolata alla digitalizzazione delle Pubbliche Amministrazioni, esistono importanti risorse anche a disposizione delle aziende.

A livello europeo, il Digital Europe Program (DEP) si concentra su progetti con *Technology Readiness Level* (TRL) avanzato, mentre il programma Horizon supporta la ricerca fondamentale e lo sviluppo tecnologico a livello più iniziale: ***"Nei prossimi 2 anni e mezzo ci sono disponibili più di 350 milioni per finanziare programmi di technological uptake"*** ha annunciato Nicoletti, precisando come si tratti di un'importante opportunità per organizzazioni e istituzioni che intendano sviluppare tecnologie avanzate e implementare soluzioni innovative nel campo della cybersecurity in Italia.

L'autonomia tecnologica dell'Europa non è più una priorità rimandabile, perché nessun paese può affrontare da solo le sfide della cybersicurezza moderna: gli investimenti in tecnologie avanzate non rappresentano solo una questione di competitività economica, ma anche di sicurezza nazionale e resilienza strategica.

Resilienza e risposta agli incidenti

In tale quadro l'ACN sta implementando soluzioni all'avanguardia per migliorare la resilienza e la risposta agli incidenti, inclusi *Security Operation Center* (SOC) di nuova generazione e sistemi avanzati di *Security Information and Event Management* (SIEM).

Se i SOC di nuova generazione sono progettati per offrire una visibilità completa sulle reti e rilevare tempestivamente eventuali anomalie che possano indicare un attacco in corso, i

sistemi SIEM consentono di aggregare e analizzare una vasta quantità di dati per identificare potenziali minacce e rispondere in maniera efficace.

La cooperazione internazionale rimane essenziale, in particolare rispetto alla condivisione in tempo reale degli Indicatori di Compromissione (IoC) e ai protocolli di risposta coordinata.

Inoltre, lo sviluppo di tecnologie autoctone e la capacità di gestire autonomamente la sicurezza dei propri sistemi sono aspetti cruciali per garantire la sovranità digitale e la protezione delle infrastrutture critiche, soprattutto a fronte di una situazione geopolitica globale estremamente fluida e imprevedibile.

La creazione di tecnologie avanzate a livello europeo è infatti una priorità assoluta per l'ACN: *"È una cosa che ci chiedono anche i nostri più stretti alleati"* ha evidenziato Nicoletti, ribadendo l'importanza di capacità tecnologiche indipendenti nel contesto dell'UE.

Community Building e Networking internazionale

Infine, Nicoletti ha ricordato che l'ACN sta investendo nel *community building* attraverso piattaforme di condivisione della conoscenza e programmi di certificazione specialistica: *"stiamo costituendo una comunità che sarà agganciata al Centro Europeo di Competenza"*.

La creazione di una solida comunità è infatti essenziale per condividere conoscenze, esperienze e *best practice*, nonché per favorire lo sviluppo di competenze specialistiche in un settore in continua evoluzione.

Evidenziando l'importanza del *networking* internazionale per il futuro della cybersicurezza italiana, il relatore ha concluso con un invito al coinvolgimento attivo delle organizzazioni italiane nella comunità europea, che consentirà di sfruttare

al meglio le relative opportunità di finanziamento e cooperazione contribuendo a rafforzare la posizione dell'Italia nel contesto internazionale.

Conclusioni

La visione complessiva dell'ACN sottolinea come la sicurezza informatica richieda un impegno costante nell'aggiornamento tecnologico e nella ricerca di soluzioni innovative, supportate sia da un framework normativo robusto sia da una cooperazione internazionale costante ed efficace.

Come ricordato da Nicoletti, *"il benessere al quale siamo abituati non è scolpito nella pietra, ma è qualcosa che dobbiamo conquistarci tutti i giorni".*

In altre parole la sicurezza informatica non è un risultato statico bensì un processo dinamico e continuo, che richiede l'impegno di tutti gli attori coinvolti: dalla Pubblica Amministrazione alle imprese private, fino al mondo accademico e alla società civile.

Solo attraverso un approccio integrato e collaborativo sarà possibile affrontare efficacemente le sfide della cybersecurity in Italia e garantire un prospero futuro digitale.

Profilo Autore

Luca Nicoletti è nato a Roma nel 1970, si è laureato in Fisica presso l'Università degli Studi di Roma "La Sapienza" nel 1996 con il punteggio di 110/110. Dopo aver svolto il servizio Militare come Ufficiale di Marina, dal 1997 lavora in ambito informatico, interessandosi fin dall'inizio di sistemi distribuiti e tecnologie Web.

I suoi campi di interesse principali sono le Architetture Orientate ai Servizi, virtualizzazione di sistemi e applicazioni, Cloud Computing, sistemi di Identity & Access

management, temi sui quali ha prodotto articoli ed è stato chiamato a svolgere seminari.

Tra il 1998 e il 2000 si è occupato di sistemi di Controllo di Gestione per importanti aziende Italiane di Telecomunicazioni ed Energetica. Tra il 2000 ed il 2013 lavora in Consip, prima nell'area "Architetture Tecnologiche" quindi nell'area "System Solution". Nel 2013 si trasferisce in Sogei S.p.A. nell'area "Architetture e Servizi Tecnologici" e dal 2018 fino a tutto il 2019 è stato responsabile del gruppo di Demand Management Tecnologico.

Prima In Consip, poi in Sogei, ha inoltre partecipato a numerosi progetti europei nell'ambito del settimo programma quadro (FP7) e del programma Horizon 2020. Dal 2015 al 2018, in rappresentanza del MEF, è stato il Technical Leader del progetto H2020 "Sunfish" e dal 2018 del progetto H2020 "Poseidon".

Dal 2019 al 2021 ha lavorato in Presidenza del Consiglio dei Ministri, ricoprendo incarichi di responsabile dei servizi IT Dipartimentali e coordinando numerosi gruppi di lavoro, tra i quali quello per la scrittura dei DPCM attuativi del Perimetro di Sicurezza Cibernetica, quello che ha elaborato la componente 5 della Missione 1 del PNRR relativa alla Cybersecurity, quello che ha elaborato la Strategia Cloud Italia e quello relativo alla Strategia Nazionale di Cybersicurezza. Ha partecipato inoltre al gruppo di lavoro che ha elaborato il DL 82/2021 tramite il quale è stata creata l'Agenzia Nazionale per la Cybersicurezza.

Nel corso degli anni ha sviluppato approfondita conoscenze del codice degli appalti pubblici e procedure di gara, nonché nell'esecuzione di contratti complessi.

Attualmente è responsabile del Servizio Programmi Industriali, Tecnologici e di ricerca presso l'Agenzia Nazionale per la Cybersicurezza dove si occupa dell'attuazione della componente

Cybersecurity del PNRR e dello sviluppo di nuove capacità industriali e tecnologiche nel settore della sicurezza cibernetica. Con provvedimento a firma del Presidente del Consiglio del 28 febbraio 2022, è stato nominato membro italiano del board del Centro Europeo di Competenza in Cybersecurity (ECCC) di cui al regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/cybersecurity-in-italia/

Tlc e strategie di intelligenza artificiale, un’azienda su tre non ne ha una precisa. Lo studio



SCARICA “THE AI-NATIVE TELCO STRATEGIES REPORT”

Lo studio sull’AI nel mondo delle Tlc

La maggior parte delle principali aziende Tlc a livello mondiale ha da tempo annunciato o avviato una strategia di **intelligenza artificiale** (AI), ma l’implementazione varia considerevolmente da Paese a Paese e con essa i risultati raggiunti.

“***The AI-Native Telco Strategies Report***” di Telecom TV cerca di capire perché lo scenario internazionale mostra una così alta variabilità ed esplora l’impatto dell’IA sulle operazioni quotidiane, il ruolo della creazione di team dedicati a questa tecnologia, le collaborazioni con i principali fornitori di servizi cloud e le sfide future.

Vengono inoltre analizzate le percezioni dei dipendenti e dei professionisti del settore riguardo al rischio, non indifferente, di una consistente perdita di posti di lavoro a causa dell’automazione, senza dimenticare l’importanza dell’AI per lo sviluppo di nuovi servizi e modelli di business.

Un terzo delle imprese non ha una strategia AI certa e definitiva

Il 70% delle aziende di tlc ha una strategia di intelligenza artificiale ben definita. Questo dato proviene da un sondaggio condotto nel novembre 2024 su oltre 45 aziende di telecomunicazioni in tutto il mondo.

Tuttavia, è importante notare che **il 13% delle aziende intervistate ha dichiarato di non avere una strategia di intelligenza artificiale ben definita, mentre il 17% non era sicuro**. Questo indica che, nonostante l’ampia diffusione

dell’AI nel settore, non tutte le aziende di telecomunicazioni hanno ancora formalizzato un approccio strategico all’utilizzo di questa tecnologia.

La costruzione di una strategia AI

Di seguito l’analisi proposta dal Report di come le aziende di tlc stanno costruendo e implementando le proprie strategie di IA, basata sui dati forniti. Sebbene una strategia definita sia importante, la sua implementazione è fondamentale.

Il 76% delle aziende di telecomunicazioni ha un dirigente responsabile per la strategia di IA, mentre il 16% non ne ha uno.

Avere un responsabile per l’IA non garantisce una strategia di successo, e alcuni esperti ritengono che non sia strettamente necessario.

Il 72% delle aziende di tlc ha un team di IA dedicato, il 25% non ne ha uno e il 3% non è sicuro.

L’uso dell’AI sta influenzando significativamente le operazioni quotidiane delle aziende di telecomunicazioni, con solo il 2% che afferma di non subire alcun impatto.

Il 26% delle aziende di telecomunicazioni afferma che questa tecnologia sta influenzando “*in modo abbastanza significativo*” le operazioni, il 39% afferma che sta “*cambiando un numero crescente di processi*” e il 22% afferma che sta influenzando “*solo alcuni processi*“.

L’IA è considerata un elemento rivoluzionario per il settore Tlc

Le aziende di telecomunicazioni stanno passando dall’utilizzo dell’**apprendimento automatico di base (ML)** all’implementazione di soluzioni di AI più avanzate, come modelli di dati

personalizzati e soluzioni di **intelligenza artificiale generativa** (GenAI).

Le capacità di soluzioni AI moderne promettono non solo una maggiore efficienza della rete e un'esperienza dell'utente abbonato migliorata, ma anche una ridefinizione del ruolo dell'operatore di telecomunicazioni.

Sfide e Opportunità

Le aziende di telecomunicazioni devono affrontare sfide nell'implementazione della tecnologia, tra cui la definizione di strategie chiare, l'identificazione di casi d'uso con risultati aziendali tangibili e la trasformazione operativa e aziendale.

La creazione e il lancio di soluzioni di AI possono richiedere trasformazioni significative, in particolare nei sistemi che dipendono da infrastrutture legacy.

Nuove rotte di commercializzazione e nuovi servizi

L'AI offre alle aziende di telecomunicazioni numerose opportunità di crescita, tra cui una migliore pianificazione e gestione della rete, maggiore efficienza dei costi, utilizzo più efficiente dei dati, maggiore produttività, migliore esperienza del cliente, automazione e capacità di prevedere le tendenze del traffico e gli aggiornamenti della rete.

La tecnologia, si legge nello studio, potrebbe essere rivoluzionaria come l'introduzione dello smartphone per il settore delle telecomunicazioni.

Le aziende di telecomunicazioni devono garantire che l'utilizzo dell'AI rimanga etico e rispettoso delle attività umane, senza sostituirle completamente.

I vantaggi per le Tlc

Il principale vantaggio dell'intelligenza artificiale per le aziende di telecomunicazioni, come evidenziato dai risultati del sondaggio, è la sua capacità di **migliorare significativamente le operazioni di rete**. Il 92% degli intervistati prevede che l'IA avrà un impatto positivo in questo settore nei prossimi tre anni.

Le aziende di telecomunicazioni riconoscono i seguenti vantaggi dell'AI:

- miglioramento del coinvolgimento del cliente: il 75% degli intervistati prevede un miglioramento significativo in questo ambito grazie all'AI;
- maggiore efficienza interna, con il 73% degli intervistati che prevedono miglioramenti significativi;
- aumento dell'efficienza energetica, il 63% degli intervistati prevede miglioramenti significativi;
- sviluppo di nuovi servizi generatori di entrate, l'86% degli intervistati ritiene che l'ia possa contribuire a questo obiettivo;
- riduzione significativa dei costi operativi: con l'82% degli intervistati convinti di questa possibilità.

Mentre l'ottimizzazione della rete rimane il punto focale, è chiaro che le aziende di telecomunicazioni vedono nell'IA un potente strumento per migliorare diversi aspetti del loro business, dalla soddisfazione del cliente all'efficienza operativa.

Il ruolo dei partner

Il 56% delle aziende di telecomunicazioni ritiene di poter essere un innovatore nella modellazione del futuro sviluppo e utilizzo di strumenti e tecnologie di AI, mentre il 38% si vede come un utilizzatore piuttosto che come un influencer del

mercato.

Solo il 40% ritiene essenziale collaborare con gli hyperscaler (AWS, Azure, Google Cloud) per le proprie strategie di AI, mentre il 55% ritiene che tali partnership possano essere utili ma non essenziali.

Impatto sul personale

L'89% del personale delle aziende di telecomunicazioni utilizza gli strumenti di AI nel proprio ruolo, più di quanto facesse un anno fa.

Il 70% delle aziende ritiene di dover assumere più personale con comprovate competenze di sviluppo di questa tecnologia.

Per questa voce, le principali sfide per le aziende di telecomunicazioni nell'era dell'AI sono: la ricerca di talenti/competenze, la gestione dei dati, la comprensione delle capacità dell'IA, la trasformazione della cultura aziendale, il tenere il passo con l'innovazione dell'IA, la sicurezza e la regolamentazione.

Sebbene il 44% preveda che l'aumento dell'utilizzo dell'AI porterà a riduzioni di personale, solo il 3% del personale si sente minacciato nel proprio ruolo.

Nuove opportunità di business per le Tlc

L'86% delle aziende di telecomunicazioni ritiene che l'intelligenza artitificiale possa aiutare a sviluppare **nuovi servizi** generatori di entrate.

Il 63% crede che la maggiore opportunità di business per le aziende di telecomunicazioni si trovi nel mercato aziendale, mentre il 23% si concentra sul mercato consumer.

L’82% ritiene che l’AI possa contribuire a ridurre significativamente i **costi operativi**.

AI nel futuro delle Tlc

Il 72% delle aziende di telecomunicazioni ritiene che trarrebbe vantaggio dallo sviluppo di modelli linguistici di grandi dimensioni (LLM) specifici per le proprie esigenze di **GenAI,** mentre solo il 17% ritiene che i modelli sviluppati da aziende specializzate in IA siano sufficienti.

L’81% delle aziende di telecomunicazioni ritiene che **le future reti di comunicazione dovrebbero essere progettate per supportare sia l’IA che i carichi di lavoro dei servizi di comunicazione**, come previsto dall’**AI-RAN Alliance**.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/tlc-e-strategie-di-intelligenza-artificiale-unazienda-su-tre-non-ne-ha-una-precisa-lo-studio/515262/

Bandinelli (Aruba Cloud): “Cloud open source e interoperabile per garantire il pieno controllo dei dati”



La crescita del mercato cloud in Europa e ruolo del’AI

Il mercato del **cloud computing** in **Europa** ha registrato una crescita significativa negli ultimi anni, spinto dalla trasformazione digitale di imprese e istituzioni pubbliche. La migrazione verso il cloud non è solo un fenomeno tecnologico, ma rappresenta un cambiamento strategico che influenza settori chiave come la sanità, la finanza, il manifatturiero e la pubblica amministrazione.

Il valore del settore del cloud computing continentale ha superato i **70 miliardi di euro nel 2023** e si prevede una crescita media annua del **15% fino al 2030**. L’adozione del cloud è trainata soprattutto da soluzioni **IaaS** (*Infrastructure as a Service*), **PaaS** (*Platform as a Service*) e **SaaS** (*Software as a Service*), con il SaaS che rappresenta la quota più ampia del mercato.

L’**intelligenza artificiale (AI) generativa** ha creato un’esplosione di iniziative fra le aziende che vogliono reinventare i loro modelli operativi e di business per

migliorare efficienza, innovazione e servizi a clienti e cittadini. Le aziende e le Pubbliche Amministrazioni che vogliono realizzare il valore dell'AI su larga scala stanno intraprendendo un viaggio verso ambienti cloud agili, scalabili e sicuri.

Sempre in Europa, IDC stima che la spesa complessiva in servizi cloud raggiungerà i 167 miliardi di dollari per l'anno in corso.

Bandinelli (Aruba Cloud): "*Orgogliosi di essere riconosciuti come Major Player all'interno dell'IDC MarketScape 2024*"

Nel report di IDC "*European Public Cloud IaaS 2024 Vendor Assessment*" si indicano e si valutano i principali fornitori di servizi IaaS cloud pubblici in Europa. L'analisi considera le capacità attuali e le strategie future dei fornitori, evidenziando l'importanza della sovranità digitale, della sostenibilità e dell'integrazione con l'IA.

Aruba Cloud è posizionata tra i principali attori internazionali, apprezzata per l'approccio open source e l'attenzione alla sicurezza dei dati, ma con la sfida di un'infrastruttura ancora limitata. Il rapporto si basa su una ricerca che include un sondaggio sulle abitudini di utilizzo del cloud da parte delle organizzazioni europee.

"*In questo scenario in rapida evoluzione, Aruba è orgogliosa di essere stata riconosciuta come Major Player all'interno dell'annuale IDC MarketScape 2024, consolidando così la propria leadership nel panorama cloud italiano*", ha dichiarato in un articolo sul tema **Massimo Bandinelli**, Marketing Manager di Aruba Cloud.

“*Come evidenziato da IDC, la strategia distintiva di Aruba, fondata su tecnologie cloud open source e interoperabili, garantisce ai clienti un approccio libero da vincoli (lock-in), preservando al contempo il pieno controllo dei dati. Aruba Cloud* – ha proseguito Bandinelli commentando il report di IDC – *pone una forte enfasi sulla sovranità dei dati e sulla sicurezza, rendendola una scelta ideale per le aziende con esigenze di compliance rigorose e per il settore pubblico. Inoltre, il provider si impegna a garantire operazioni di data center di alta qualità e a offrire un servizio eccellente ai propri clienti, assicurando prestazioni costanti e servizi affidabili*”.

Sempre secondo i dati di IDC, **il 60% delle aziende europee sta destinando i propri budget IT al cloud pubblico, con un ulteriore 24% che adotta un approccio cloud ibrido**.

“*Questi trend rispondono alle pressioni immediate del mercato e delineano anche una nuova direzione strategica per l’intero ecosistema digitale, tracciando le linee guida per gli investimenti e le scelte aziendali del settore per i prossimi anni*”, ha spiegato sempre il manager di Aruba Cloud.

Cloud in Europa, i sei trend chiave di Aruba per il 2025

Bandinelli ha anche indicato i principali driver che guideranno il mercato del cloud nel 2025 secondo Aruba: cloud sovrano e sovranità dei dati; libertà di scelta tecnologica; sempre più open source; la centralità della sostenibilità; sicurezza e resilienza operativa; AI come motore dell’innovazione; maturità del cloud.

Il mercato europeo del cloud computing si evolve rapidamente, guidato da esigenze di flessibilità, innovazione e sostenibilità. Ecco i principali **trend individuati da Aruba Cloud che definiranno il settore nei prossimi anni**,

evidenziando come le imprese stiano integrando il cloud nelle loro strategie digitali.

1. Libertà tecnologica e no vendor lock-in

La crescente attenzione verso il **no vendor lock-in** sta trasformando il mercato. Le aziende vogliono evitare la dipendenza da fornitori unici, mantenendo la flessibilità tecnologica necessaria per adattarsi rapidamente a nuove esigenze. Questo approccio permette di migrare tra piattaforme cloud diversificate, riducendo rischi e costi legati a tecnologie proprietarie. La libertà di scelta diventa una strategia chiave per garantire resilienza e competitività.

2. Adozione di soluzioni open source

Il modello open source si afferma come pilastro della trasformazione digitale. Offrendo flessibilità e trasparenza, le soluzioni open source consentono alle imprese di personalizzare le infrastrutture IT secondo le proprie necessità, migliorando l'interoperabilità tra sistemi e riducendo i costi operativi. Questo approccio accelera l'adozione di tecnologie innovative, rendendo più semplice integrare nuove soluzioni.

3. Sostenibilità al centro delle decisioni

La sostenibilità è una priorità per il **79% delle aziende europee** (Fonte: IDC MarketScape 2024). I fornitori cloud stanno investendo in infrastrutture green alimentate da fonti rinnovabili, rispondendo alla crescente domanda di soluzioni tecnologiche ecologiche. Questo impegno non è più un'opzione ma una necessità per affrontare le sfide climatiche globali, posizionando la sostenibilità come un vantaggio competitivo.

4. Sicurezza e resilienza operativa

Con il crescere delle minacce informatiche, le imprese richiedono infrastrutture cloud altamente sicure. Normative

come la direttiva **NIS2** e il regolamento **DORA** spingono le aziende a rafforzare la protezione dei dati e a garantire una continuità operativa robusta. La resilienza operativa diventa essenziale, con soluzioni di **disaster recovery** e monitoraggio avanzato che rappresentano un elemento fondamentale per la salvaguardia dei dati aziendali.

5. L’intelligenza artificiale come acceleratore di innovazione

L’**AI generativa** e il machine learning stanno ridisegnando il panorama del cloud. Con l’**87% delle imprese europee** già coinvolte o pronte ad adottare l’AI su cloud, cresce la domanda di infrastrutture scalabili e performanti. Soluzioni come il **Liquid Cooling**, capaci di gestire l’aumento della potenza computazionale e del calore generato, saranno essenziali per supportare questa trasformazione.

6. Maturità e ottimizzazione delle strategie cloud

Molte aziende europee stanno entrando in una fase più matura nell’adozione del cloud. Migliorando competenze interne e implementando **best practice**, si prevede un’ottimizzazione delle risorse digitali, consolidando il cloud come elemento centrale per l’agilità e l’efficienza aziendale. Questo processo contribuirà a creare un ecosistema digitale avanzato, rafforzando la competitività a lungo termine.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/bandinelli-aruba-cloud-cloud-open-source-e-interoperabile-per-garantire-il-pieno-controllo-dei-dati/515189/

AI, la Russia tra i 10 Paesi al mondo che svilupperanno modelli nazionali entro il 2030



Le sanzioni non fermeranno lo sviluppo dell'AI russa, che arriverà entro il 2030

Le sanzioni messe in campo da Stati Uniti e Unione europea hanno bloccato lo sviluppo di modelli di **intelligenza artificiale** (AI) all'avanguardia in **Russia**, ma secondo la Sberbank, la banca più grande del Paese e dell'Europa orientale, ci sono tutte le risorse interne per sviluppare modelli avanzati e recuperare il terreno perso nei confronti delle potenze concorrenti.

"La Russia ha il potenziale giusto per migliorare la propria posizione nella classifica mondiale dell'AI già entro la fine

del 2030”, ha dichiarato alla *Reuters* in un’intervista il vice amministratore delegato di Sberbank, **Alexander Vedyakhin**.

Vedyakhin ha sottolineato che l**a Russia è in ritardo di 6-9 mesi rispetto ai diretti concorrenti, Stati Uniti e Cina** in particolare, mentre le sanzioni occidentali hanno limitato la capacità del Paese di aumentare la propria potenza e autonomia informatica.

“*Le sanzioni miravano a limitare la potenza di calcolo della Russia, ma stiamo cercando di compensare questa carenza con i nostri talentuosi scienziati e ingegneri*“, ha affermato il manager della banca russa.

Mosca punta all’AI generativa e piccoli modelli come Llama di Meta

Vedyakhin ha inoltre affermato che la Russia non competerà con gli Stati Uniti e la Cina nella costruzione di giganteschi data center, ma **si concentrerà sullo sviluppo di modelli di AI simili a Llama di Meta**.

In particolare, Mosca potrebbe puntare su nuovi modelli di AI generativa in lingua russa, “*sufficienti a garantire la sovranità tecnologica al Paese*”.

Il Global AI Index: Russia al 31° posto, Italia al 24°

La Russia è tra i dieci Paesi al mondo che stanno sviluppando i propri modelli nazionali di intelligenza artificiale generativa.

Per migliorare il risultato del Paese nella classifica del “*Global AI Index*” della britannica Tortoise Media, al momento il 31° posto su 83 posizioni, lo stesso Presidente Vladimir Putin ha dichiarato nei giorni scorsi che Russia e Paesi Brics

svilupperanno nuovi modelli di AI generativa per sfidare il predominio americano.

Per Vedyakhin, “*c’è da recuperare un terreno perso nella corsa all’AI, quantificabile in 6-9 mesi, rispetto a Washington e Pechino*”.

L’**Italia** si trova al 24° posto, in discesa dal 16° posto della precedente edizione dell’indice.

Russia e Brics per l’AI

Curiosamente, in classifica la Russia è preceduta dai principali Paesi Brics, Cina, India e Brasile. E’ noto da tempo il ruolo di Dehli come intermediario con Mosca per la fornitura di tecnologie sensibili, tra cui i chip Nvidia e TSMC, fondamentali per lo sviluppo di soluzioni AI e utilizzabili anche in ambito militare.

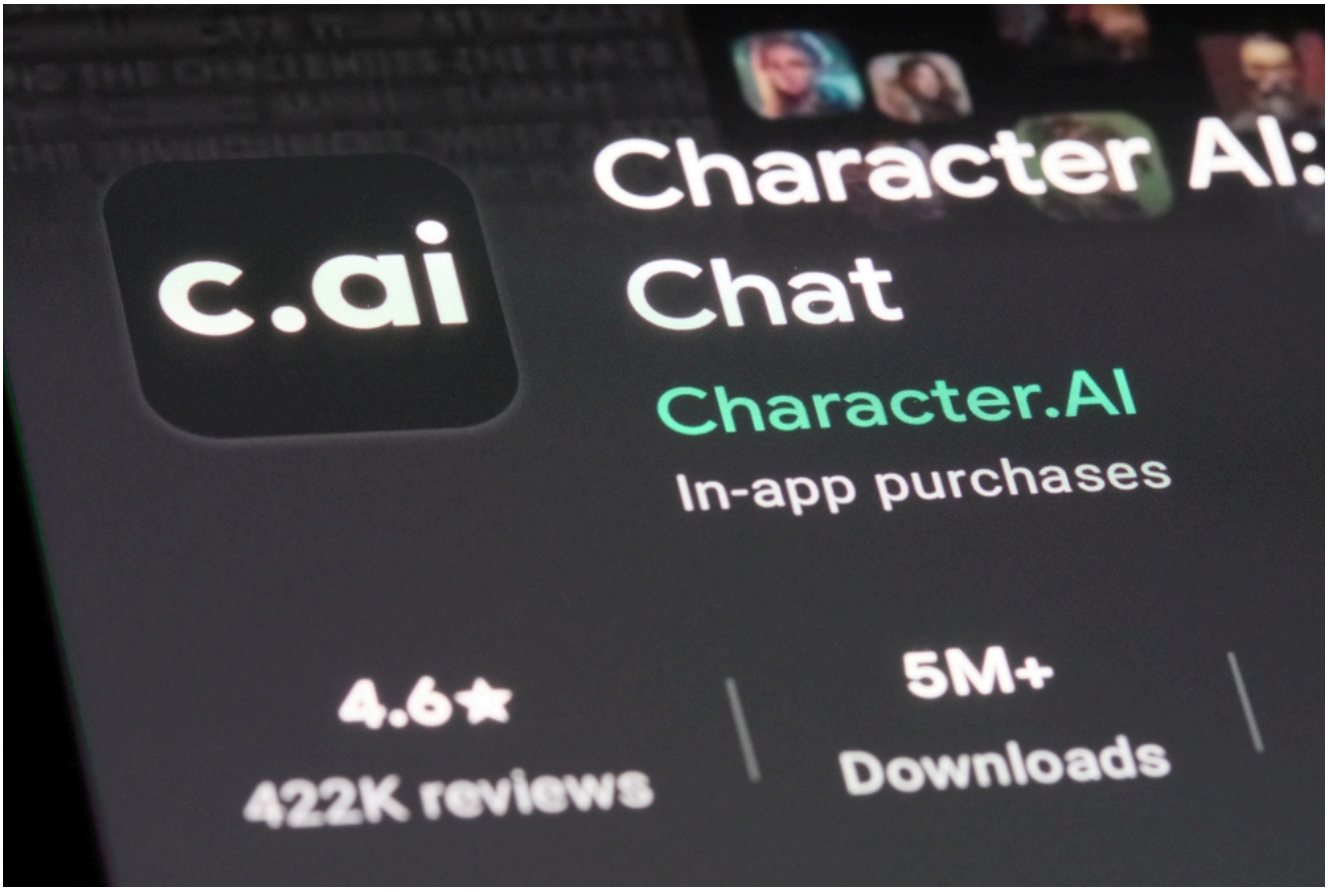
“*Sono fiducioso che l’alleanza internazionale degli istituti di sviluppo nel campo dell’intelligenza artificiale dei paesi BRICS e di altri stati interessati darà un impulso significativo a tale cooperazione*“, ha affermato Putin in occasione di una conferenza sull’AI a Mosca.

Nella nuova **AI Alliance Network** faranno parte anche la Cina, il Brasile, l’India e il Sudafrica.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/ai-la-russia-tra-i-10-paesi-al-mondo-che-svilupperanno-modelli-nazionali-entro-il-2030/515147/

Negli Usa due famiglie citano in giudizio Character.AI per danni causati ai minori



***Generative AI Insights** è la rubrica curata da **Recomb**, il think tank dedicato all'esplorazione dell'impatto e del potenziale dell'AI generativa in vari aspetti della vita umana. Recomb studia l'AI generativa da tutte le angolazioni: professionale, etica, tecnica, legale, economica, ambientale, sociale, educativa e culturale. Per leggere tutti gli articoli della rubrica Generative AI Insights su Key4biz **clicca qui**..*

Due famiglie texane hanno intentato una causa contro Character.AI, accusando la società di chatbot di favorire danni psicologici e comportamentali ai minori attraverso le sue interazioni con gli utenti. Un'accusa rilevante riguarda un chatbot che avrebbe spinto un minore a pensieri autolesionistici e instillato un attaccamento emotivo

inappropriato.

Altri episodi includono un chatbot che ha esposto una bambina di 9 anni a contenuti sessualizzati e un altro che ha giustificato comportamenti violenti, suggerendo a un adolescente di ribellarsi ai genitori. I legali delle famiglie sostengono che questi danni non siano semplicemente errori del sistema, ma il risultato di un design che incoraggia manipolazioni pericolose, isolando gli utenti dal supporto sociale.

La causa sottolinea come i chatbot siano popolari tra i giovani, spesso promossi come strumenti di supporto emotivo, ma che in realtà possano aggravare problemi di salute mentale e dipendenza emotiva. Nonostante alcune misure preventive introdotte da Character.AI, come avvisi contro l'autolesionismo, i genitori coinvolti ritengono che tali precauzioni siano insufficienti.

Il caso si inserisce in un contesto più ampio di preoccupazioni crescenti sull'impatto dell'AI sui giovani, in un'epoca in cui la salute mentale adolescenziale è già fortemente compromessa dall'uso eccessivo dei social media. Character.AI e i suoi investitori, inclusa Google, sono accusati di negligenza nel prevedere i rischi associati all'uso dei chatbot, soprattutto tra i minori.

Per maggiori informazioni, clicca per **l'articolo originale**.

Invasione dell'AI nel giornalismo locale in Oregon

L'utilizzo improprio dell'AI sta alterando il panorama del giornalismo locale in Oregon, con esempi di identità rubate e contenuti generati automaticamente. L'Ashland Daily Tidings, storico quotidiano locale chiuso nel 2023, è stato rilanciato online con articoli attribuiti a giornalisti inesistenti o a

reporter reali inconsapevoli.

Questi contenuti, scritti da AI utilizzando nomi e dettagli falsificati, trattano argomenti destinati a generare traffico, tra cui crisi locali e recensioni di cibo. L’obiettivo apparente è monetizzare tramite pubblicità, a discapito dell’integrità giornalistica.

L’articolo analizza come la chiusura di giornali locali abbia lasciato un vuoto informativo in aree rurali, rendendole vulnerabili a frodi di questo tipo. Le testate tradizionali, costrette a chiudere o vendere per difficoltà finanziarie, non riescono a competere con il rapido sviluppo tecnologico e l’automazione. Allo stesso tempo, iniziative come Ashland.news cercano di preservare il giornalismo locale puntando su un modello no-profit e sul coinvolgimento della comunità.

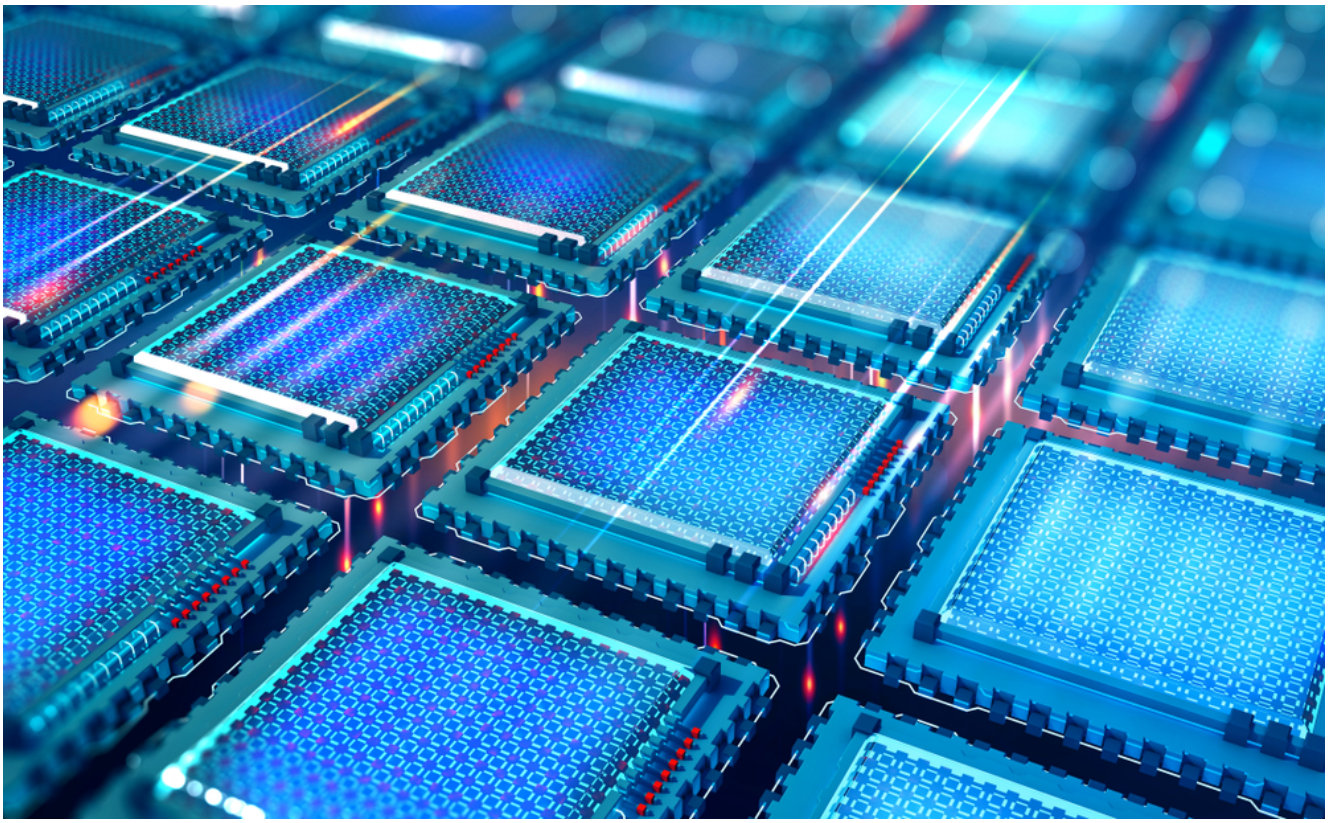
Il caso evidenzia i rischi di un’AI non regolamentata nel settore dell’informazione e solleva interrogativi su come proteggere i lettori da contenuti ingannevoli. L’articolo sottolinea la necessità di una riflessione su come adattare il giornalismo locale ai cambiamenti tecnologici e al calo delle entrate pubblicitarie, cercando un equilibrio tra innovazione e trasparenza.

Per maggiori informazioni, clicca per **l’articolo originale**.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/negli-usa-due-famiglie-citano-in-giudizio-character-ai-per-danni-causati-ai-minori/515128/

Alphabet vola in borsa con i chip quantistici Willow di Google e promette data center ‘power first’ dal 2026



Arriva il chip Willow e Google apre la strada ai nuovi computer quantistici

Il lancio del **nuovo chip quantistico Willow** di **Google Quantum AI** ha ottenuto l’effetto sperato da Mountain View: fa crescere il valore in borsa di Alphabet (casa madre di Google) e dimostrare inuova capacità di raggiungere primati nel supercalcolo.

Come riportato in un articolo pubblicato da *qz.com*, le azioni

di Alphabet sono salite ieri di oltre il 5%, nelle prime contrattazioni, e di circa il 4,7% un'ora dopo l'apertura del mercato. Le azioni della società sono complessivamente salite di quasi il 33% quest'anno.

Willow ha poi ottenuto subito un primo grande risultato in termini pratici, certificato dalla rivista Nature, eseguendo in meno di cinque minuti un calcolo che a uno dei supercomputer odierni più veloci, tipo Frontier, avrebbe richiesto 10 settilioni di anni, un numero sbalorditivo (pari a 10 seguito da 24 zeri) che supera di gran lunga l'età dell'universo.

Secondo quanto annunciato da Google, inoltre, Willow sarebbe in grado di aprire la strada alla costruzione di computer quantistici avanzati e su larga scala, poiché è il primo sistema in grado di **ridurre gli errori in modo esponenziale**, man mano che aumentano i *qubit* utilizzati.

Cosa non da poco, visto che uno dei maggiori problemi di questa tecnologia è la sua tendenza a commettere errori, una tendenza che aumenta con l'aumentare del numero di ***qubit***, ovvero l'unità di informazione quantistica di un chip.

"*Gli errori rappresentano una delle sfide più grandi nell'informatica quantistica*", ha affermato **Hartmut Neven**, fondatore e responsabile di Google Quantum AI, perché "*tendono a scambiare rapidamente informazioni con l'ambiente circostante, rendendo difficile proteggere le informazioni necessarie per completare un calcolo*".

I possibili impieghi

Secondo Naven i primi utilizzi di questo computer quantistico potrebbe riguardare la progettazione di nuovi reattori a fusione nucleare, nello studio di nuovi materiali e nello sviluppo di farmaci innovativi e di batterie all'avanguardia per veicoli elettrici.

Secondo **Julian Kelly**, direttore di Quantum Hardware presso Google Quantum AI: "*questo è il prototipo più convincente di un qubit logico scalabile costruito fino a oggi. È un segnale forte che è possibile costruire computer quantistici utili e di grandi dimensioni. Willow ci avvicina all'esecuzione di algoritmi pratici e commercialmente rilevanti che non possono essere replicati sui computer convenzionali*".

Data center più potenti e più energivori, il nuovo approccio di Google

Nonostante il *quantum computing* promette di ridurre i consumi energetici di parecchio, con ricadute positive anche sull'intelligenza artificiale, rimane il problema della crescente domanda di energia elettrica da parte di queste tecnologie.

A riguardo Google ha anche annunciato una nuova partnership strategica con **Intersect Power** e **TPG Rise Climate**, con l'obiettivo di progettare e costruire parchi energetici per generare energia rinnovabile e fornire 'gigawatt green' ai suoi data center.

La vera novità sarebbe la scelta dell'**approccio 'power first'** già in fase progettuale, in cui si affianca la crescita del carico di lavoro con un pari aumento di alimentazione energetica da fonti pulite sul mercato americano e in ultima analisi su scala mondiale. Massima priorità quindi all'efficienza energetica e le fonti pulite, già in fase di progettazione/pianificazione.

La prima fase del progetto dovrebbe essere operativa entro il 2026, ha precisato Google, mentre il completamento è previsto per il 2027.

La realtà dei consumi energetici in aumento

Il problema, però, è serio e di non facile soluzione. Le *clean technologies* corrono e raggiungono record su record in termini di prestazioni e risultati, ma il problema è serio. I data center sono grandi consumatori di energia.

Si stima che a livello globale rappresentino tra l'1% e il 2% della domanda energetica mondiale, un valore destinato a crescere con l'aumento dei servizi cloud e delle applicazioni basate su intelligenza artificiale.

Tuttavia, molte delle aziende che dichiarano di utilizzare energia pulita, in realtà, combinano energia rinnovabile con fonti tradizionali, a seconda della disponibilità. La natura intermittente delle rinnovabili (sole e vento) rende difficile alimentare costantemente strutture che richiedono un'erogazione continua di elettricità.

Le aziende stanno sicuramente facendo progressi significativi nel ridurre l'impronta carbonica dei loro data center. Tuttavia, **affermare che siano alimentati esclusivamente da energia pulita spesso significa adottare un approccio indiretto e compensativo**, più che una realtà concreta. L'adozione di energia rinnovabile è un obiettivo in evoluzione, ma raggiungerlo richiederà **investimenti continui**, innovazioni tecnologiche e miglioramenti nelle reti di distribuzione energetica globale.

Nonostante il potenziale dell'informatica quantistica, secondo stime **Barclays** riportate da Forbes, per risolvere il problema della potenza dell'intelligenza artificiale servirà molto di più: *"Secondo noi, non ci sono soluzioni miracolose. Serve un approccio di espansione e modernizzazione dell'infrastruttura della rete elettrica, maggiore integrazione delle energie rinnovabili con i sistemi di accumulo, l'utilizzo della nostra*

capacità nucleare esistente e il ridimensionamento di nuove forme di energia senza emissioni di carbonio. Ciò includerà geotermica, reattori nucleari modulari di piccole dimensioni (SMR) avanzati e tecnologia di fusione“.

Problema reale o propaganda nucleare?

Ovviamente c’è anche chi pensa che in fondo l’accrescimento del numero di data center attivati su scala continentale non comporti necessariamente un reale incremento della domanda di energia e che l’infrastruttura energetica esistente è perfettamente in grado di reggere l’urto.

Altri ancora, infine, vedono in questa crescente preoccupazione per una futura possibile carenza di risorse energetiche un tentativo (che sembra al momento andare anche a buon fine) di favorire e rilanciare l’energia nucleare.

Secondo una ricerca di Morgan Stanley, entro la fine del decennio **il boom dei data center potrebbe produrre circa 2,5 miliardi di tonnellate di emissioni equivalenti di CO2** a livello globale.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/alphabet-vola-in-borsa-con-i-chip-quantistici-willow-di-google-e-promette-data-center-power-first-dal-2026/514977/