PARTNERS • NUMERO 63

PARTNERS

INFORMAZIONE E FORMAZIONE PER IL CANALE A VALORE

OPEN INNOVATION

l'azienda al centro di un ecosistema di partner

MARKET REVIEW

STAMPA CONNESSA ELEMENTO CHIAVE NELLA DIGITAL TRANSFORMATION

snom

Soluzioni IP ottimizzate per ogni esigenza!

Con oltre 25 anni di esperienza nel campo della telefonia aziendale, Snom offre soluzioni su misura per ogni ambiente e ogni esigenza: che si tratti di call center, home office o ufficio classico, il nostro obiettivo è quello di offrirvi sempre la soluzione ottimale per il vostro progetto. Potete contare su di noi!

www.snom.com

SOMMARIO

SETTEMBRE 2024 • N. 63

PARTNERS
Anno XIII - numero 63
Settembre 2024

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

Hanno collaborato: Maurizio Ferrari, Fabrizio Pincelli, Leo Sorge, Stefano Uberti Foppa

Redazione:
REPORTEC srl | Via Gorizia 35/37
20099 Sesto San Giovanni (MI);
Tel 02 24304434 | www.reportec.it |
redazione@reportec.it

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

Diffusione: 35.000 copie digitali

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

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

opentext™ Cybersecurity

LA NOSTRA FORZA È LA VOSTRA SICUREZZA

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

Aviator by opentext™
IDENTIFICA
ogni minaccia con la potenza dell'intelligenza artificiale

NetIQ by opentext™
GOVERNA
l'accesso e l'identità con una gestione Zero Trust

Voltage by opentext™
PROTEGGI
la privacy e i dati strutturati e non strutturati

ArcSight by opentext™
BLOCCA
ogni tipo di minaccia e rispondi in modo rapido e proattivo

Fortify by opentext™
RAFFORZA
la sicurezza delle applicazioni con analisi del codice e test

opentextcybersecurity.it

RICCARDO FLORIO
DIRETTORE RESPONSABILE

Dall'AI generativa ai robot antropomorfi: la fantascienza dietro l'angolo

Negli ultimi diciotto mesi, il mercato delle tecnologie, sia informatiche che non, è stato dominato dal tema dell'intelligenza artificiale generativa. Questo fenomeno, **più che essere il risultato di una singola innovazione tecnologica, è stato spinto dall'introduzione di interfacce semplici** e immediate che hanno reso l'AI accessibile a tutti. Ciò che inizialmente poteva sembrare un gioco si è rapidamente trasformato in uno strumento potente, capace di fornire indicazioni, risposte e contenuti utili sia per il lavoro che per la vita quotidiana. È difficile trovare qualcuno che, dopo aver provato l'AI generativa, non sia rimasto impressionato dalla sua potenzialità.

L'intelligenza artificiale offre suggerimenti e informazioni su una vasta gamma di argomenti, senza essere limitata a un settore specifico. È proprio questa universalità che ne sta decretando il successo. Si tratta di una rivoluzione tecnologica che, come accaduto anni fa con la mobilità, parte dal basso ovvero dal mondo consumer e che si sta ora estendendo a quello business, alimentando investimenti enormi che accelerano lo sviluppo in modo esponenziale. L'entusiasmo generato da questa nuova tecnologia ha spinto le grandi aziende a investire miliardi, portando l'evoluzione dell'AI a ritmi incredibili. Le funzionalità si evolvono così rapidamente che, prima ancora di abituarsi a una nuova caratteristica, essa viene migliorata e potenziata.

In pochi mesi siamo passati da strumenti che fornivano semplici ri-

RICCARDO FLORIO
DIRETTORE RESPONSABILE

sposte testuali a quelli che generano immagini, video, musica, arrangiamenti e che sono in grado di accettare file e creare riassunti o elaborazioni in qualsiasi lingua. La velocità di questo sviluppo è tale che le **preoccupazioni legittime sull'impatto dell'AI si trovano spesso a essere superate dagli eventi, rendendo obsolete molte delle discussioni sul tema.**

Tra le principali preoccupazioni degli esperti vi è l'impatto dell'AI sulla sicurezza informatica. Ma non solo: molte sono le discussioni riguardanti il futuro del lavoro, con alcuni che già prevedono la scomparsa di diverse professioni o la loro profonda trasformazione.

L'impatto interesserà tutte le professioni che prevedono lavori di tipo creativo o comunque non manuale: illustratori, scrittori, giornalisti, pubblicitari, musicisti ma anche sviluppatori di software, avvocati, matematici. In un mondo in cui tutti pensano di avere qualcosa da comunicare al mondo e in cui chiunque ha la possibilità di auto pubblicare, l'AI ci condannerà anche a un aumento smisurato di libri inutili e ridondanti.

Tuttavia, vi è il concreto rischio di riporre troppa fiducia in questa tecnologia. L'AI è uno strumento di grande efficacia, ma **senza la conoscenza critica necessaria per riconoscerne gli errori, si potrebbe rischiare di incorrere in errori grossolani** e, magari, arrivare persino a posizionare Galileo Galilei come contemporaneo di Cristoforo Colombo (!).

È probabile che presto emergeranno segnali di dissenso nei confronti dell'AI, andando oltre le obiezioni ragionevoli e sfociando in un'opposizione più radicale e spesso immotivata, che potrebbe vedere nell'AI un capro espiatorio per tutti i problemi del mondo.

Dal punto di vista dello sviluppo tecnologico, i prossimi anni vedranno significativi progressi in vari ambiti. In primo luogo, ci sarà

RICCARDO FLORIO
DIRETTORE RESPONSABILE

una maggiore flessibilità e **rapidità nell'accesso alle informazioni disponibili ovunque in tempo reale.** In secondo luogo, la **qualità dell'analisi e degli algoritmi** continuerà a migliorare, permettendo all'AI di offrire feedback sempre più precisi e aggiornati. Infine, **l'integrazione dell'AI in una vasta gamma di processi, settori e dispositivi** porterà a un impatto ancora più diffuso.
Per trovare alcuni esempi in realtà basta attingere alla cinematografia di fantascienza degli ultimi decenni. Basti pensare ai traduttori simultanei (già presenti in Star Trek del 1966), che presto diventeranno realtà, permettendo traduzioni vocali in tempo reale, con voci sintetizzate indistinguibili da quelle umane. O ai tavoli medici automatizzati, capaci di effettuare in autonomia diagnosi e interventi chirurgici.
Ma il vero passo successivo sarà **l'incontro tra l'AI generativa e la robotica antropomorfa**, un concetto che per anni è rimasto confinato nell'immaginario collettivo. **Le tecnologie sono ormai mature per questa convergenza**, supportate da un incremento costante della capacità computazionale, dall'accesso sempre più ampio alla banda larga, dallo sviluppo dell'Edge computing, dall'innovazione nei sensori grazie all'IoT, dalle nuove tecnologie di miniaturizzazione dei motori, da materiali innovativi realizzati con il contributo delle nanotecnologie fino ai tessuti sintetici capaci di imitare la pelle umana.
I robot antropomorfi della fantascienza sono ormai a un passo dal diventare realtà ma, probabilmente interagiranno con l'ambiente in modo differente dal nostro. Non avranno bisogno di toccare gli oggetti per svolgere gran parte delle loro attività, utilizzare la voce per comunicare e di muoversi sulle proprie gambe per giungere in un luogo. **In un mondo in cui tutto è connesso e automatizzato potranno fare la maggior parte dei lavori restando fermi e in silenzio** e riservare le azioni più antropomorfe per far sentire più a loro agio le persone.

Open Innovation: l'azienda al centro di un ecosistema di partner

Le imprese sono in gran parte ormai strutturalmente aperte a un processo di innovazione di prodotti e servizi attraverso la relazione con i propri partner. Ma se da un lato sono numerosi e differenti i player che offrono servizi di open innovation, dall'altro serve di continuo aggiornare, in azienda, il proprio livello di permeabilità all'innovazione proveniente dall'esterno. Lavorando su processi, modelli, metriche, tecnologie e competenze, perché anticipare il mercato e creare innovazione in modo condiviso è ormai l'unica strada possibile per una business innovation

di **Stefano Uberti Foppa**

Molti passi avanti sono stati compiuti da quando nel lontano 2003, il professor Henry Chesbrough, dell'Università della California, coniò il termine "open innovation". Da allora sperimentazioni, metodologie, cambiamenti culturali sono avvenuti di continuo nelle aziende per provare a creare un'innovazione in sinergia con realtà al di fuori del classico perimetro aziendale. Saper integrare idee ma anche contaminare con processi differenti il proprio modo legacy di operare, è una sfida che, quotidianamente, le imprese devono saper affrontare.
La disruption continua dei mercati (mutamenti repentini della domanda, imprevedibilità socio-economiche, guerre e pandemie che impat-

tano sulle economie globali e locali, opportunità di business da sfruttare al volo), necessita una velocità di risposta a cui serve una flessibilità che solo un'integrazione continua con modelli di open innovation può garantire.

Le modalità sono numerose e peculiari per ogni azienda. Da una open innovation realizzata con modalità più tradizionali, svolta in prevalenza attraverso fasi di feed back continui con clienti e fornitori, a reti di partner esterni culturalmente differenti dall'impresa che vengono integrati non solo per specifici progetti ma diventano strutturali al cambiamento e a un'innovazione continua.

Tracciare una fotografia di questo fenomeno è estremamente complesso. Tuttavia, prima di focalizzare alcune linee guida anche grazie al recente studio **"Italian Open Innovation Lookout 2024"** realizzato dal gruppo di ricerca Innovation & Strategy della School of Management del Politecnico di Milano, serve mettere un punto fermo: ogni forma di open innovation è destinata a fallire se il ricorso a realtà esterne innovative non è supportato da un processo di vera integrazione. Accanto infatti a specifici progetti nei quali le aziende ricorrono a soggetti innovativi per sviluppare nuovi prodotti/servizi, serve che vi sia un "portato culturale" che impatti, almeno parzialmente, su processi e culture di impresa, sulle modalità di relazione verso l'ecosistema dei partner e verso il mercato. Per fare questo non servono solo buone intenzioni e disponibilità, ma un insieme preciso di azioni e di strumenti da implementare che possano facilitare l'interoperabilità sia interna sia esterna all'azienda con i propri partner. Strumenti, oggi tutti disponibili in cloud, di condivisione, di analisi dati, di project management, piattaforme di Ucc (Unified communication and collaboration) e soprattutto processi che si riferiscano a metodologie flessibili e collaborative in grado di accogliere l'innovazione. Processi di gestione organizzativa di impresa che fanno della flessibilità il proprio riferimento operativo. Tra questi, ad esempio, l'Agile, la metodologia dell'ingegneria del software nata nei primi anni 2000 con l'obiettivo di velocizzare e rendere qualitativamente migliore il rilascio delle applicazioni software. Si basa su un approccio poco strutturato, con team di sviluppo piccoli, poli-funzionali e auto-organizzati. Prevedendo iterazione, integrazione, miglioramenti incrementali, cambiamenti in corsa sulla base delle esigenze che di volta in volta emergevano da parte dei destinatari del software. Modelli operativi codificati che per la loro estrema flessibilità sono stati ben presto estesi dalla specificità dello sviluppo codice all'organizzazione delle business unit aziendali.

Servizi di ogni tipo per fare open innovation

Guardiamo allora ad alcuni highlight del fenomeno in Italia emergenti dal Rapporto citato. Su un campione iniziale identificato di

905 aziende che operano nel segmento dei servizi di open innovation si è svolta una mappatura che ha portato all'identificazione di 398 organizzazioni per 25 categorie di Service Provider organizzate in 10 macro-categorie che compongono il sistema italiano dell'Open Innovation. Il valore stimato è di 696 milioni di euro per i quali le categorie, poi ridotte a 15 nello studio per significatività, contribuiscono in modo differente al valore totale dei servizi di open innovation. Infatti il 30% delle 15 categorie considerate genera oltre l'85% del valore del mercato. Si tratta di un'area di player specializzati molto affollata. Vi sono Innovation Center, Società di consulenza, aziende specializzate nella gestione dei diritti di proprietà intellettuale, Problem solver focalizzati nei vari ambiti, Incubatori e Acceleratori, Venture Builders e Start-up Studio, Player Finanziari, Enti di ricerca e formazione, fino agli spazi di co-working.
Tra i principali Service Provider vi sono i Corporate Innovation Hub che con un fatturato medio di 12,6 milioni di euro, generano circa 290 milioni di euro, rappresentando oltre il 40% del valore totale del mercato. Coaching, Mentoring, Tutoring, Networking, Prototipazione, Scouting tecnologico, Consulenza strategica, supportano le aziende anche nello sviluppo di Proof of Concept e Minimum Viable Product. Seguono le Società di Consulenza che contribuiscono con circa 112 milioni di euro, pari al 16% del totale.

GLI APPROFONDIMENTI DI BIZZIT

L'inevitabile scelta dell'open innovation

Un altro studio di **Capgemini,** pubblicato nel 2023, ha offerto una panoramica significativa su cosa rappresenta, e soprattutto rappresenterà nei prossimi anni, il ricorso delle imprese agli ecosistemi di innovazione per affrontare la crescente complessità competitiva. Anche in questo caso, lo studio ha evidenziato la necessità di credere fermamente nell'importanza degli investimenti e delle trasformazioni, sia a livello di processi che di cultura aziendale, verso una reale integrazione. Questo approccio rappresenta l'unica via per raggiungere la flessibilità e la capacità di resistere alle disruption.

LEGGI LO STUDIO

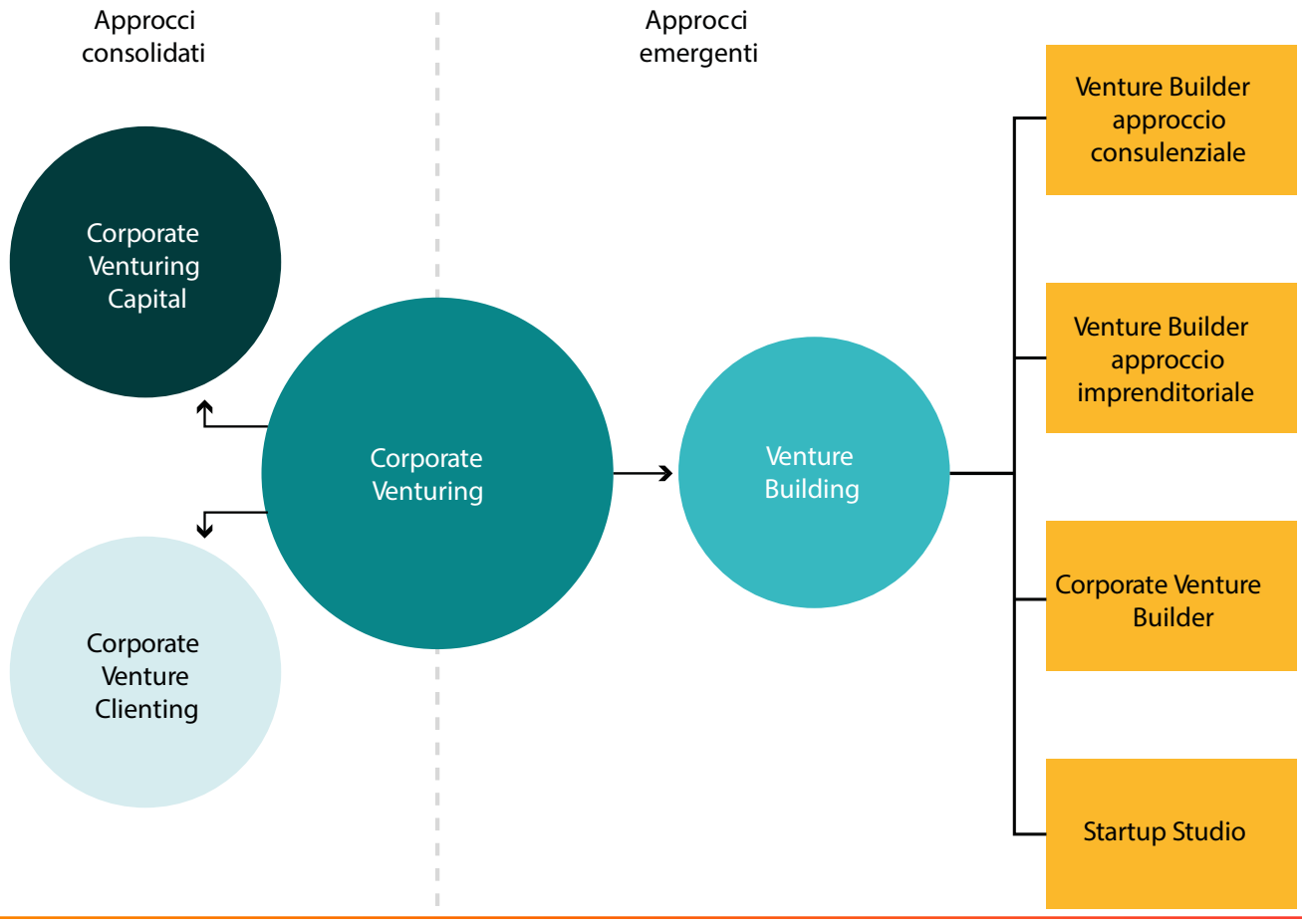
Strumenti per flessibilizzare, anticipare, cercare l'innovazione

Lo studio sottolinea il ruolo crescente del Corporate Venturing, usato dalle aziende per stimolare un processo di innovazione al di fuori delle rigide dinamiche gestionali interne, creando o sostenendo realtà imprenditoriali nei settori di interesse aziendale o in quelli emergenti per attivare uno scambio sia su progetti sia su modelli operativi. Per portare nuove capacità, contaminazione culturale e organizzativa, rinnovamento strategico e, naturalmente, business. Si tratta di fatto di ricercare nell'ampio e frammentato ecosistema delle start up quelle realtà

più idonee, quasi "su misura", per accelerare e rendere più agile il proprio processo di innovazione. In questo contesto, spiccano approcci consolidati come il Corporate Venture Capital e il Corporate Venture Clienting, a cui si affiancano però modelli emergenti quali il Venture Builder e Startup Studio (realtà che offrono soluzioni plug & play, fornendo direttamente l'accesso a una delle startup presenti a portafoglio anziché offrire un servizio di creazione di una nuova azienda) in cui è maggiore l'autonomia operativa dall'azienda madre e dai suoi processi, mantenendo tuttavia il vantaggio di maggiori sinergie. Le divisioni aziendali che si occupano di Venture Capital, puntano ad agevolare lo scambio di risorse con le start up individuate per favorire lo sviluppo progettuale. Tuttavia l'alchimia non è semplice: ancora una volta processi legacy, competenze inadeguate, prospettive e interessi diversi tra gli attori fanno sì che spesso il percorso si interrompa o si complichi molto. Scouting e valutazioni iniziali non sono fasi semplici; la gestione delle interazioni vedono lo scontro di modelli culturali molto differenti tra loro; le start up temono spesso l'appropriazione tecnologica da parte delle aziende mentre quest'ultime vedono nelle prime un approccio al mercato che non essendo facilmente strutturabile spesso si incaglia nei rapporti interpersonali, con tutti i rischi del caso. Nel Corporate Venture Clienting viene invece definita tra impresa e startup una relazione a tutti gli effetti cliente-fornitore in cui le

I MODELLI DI CORPORATE VENTURING

Fonte: "Italian Open Innovation Lookout 2024" - Politecnico di Milano



realtà si focalizzano sullo sviluppo collaborativo di tecnologie, servizi e prodotti. È maggiore la vicinanza tra i due soggetti così come l'accesso, per la start up, a risorse aziendali preziose (parziale accesso alla base clienti, team dedicati, eliminazione di livelli gerarchici nella relazione, ecc), fino al test finale del prodotto o del servizio identificato, per poi decidere l'eventualità di un investimento diretto. Fino ad arrivare, e questo è un modello che va affermandosi di recente, sottolinea lo studio, a una vera e propria creazione ex-novo di impresa indipendente (Venture Building), sempre collegata con l'azienda madre, ma con modelli operativi molto flessibili. Sono solo alcuni accenni che però rendono concreto lo sforzo delle imprese nel ricercare vie di innovazione. Ma nonostante strumenti e strategie, spesso questo processo si ferma, non decolla. Un po' perché nell'open innovation il fallimento è un elemento strutturale, altamente probabile. E un po' perché le imprese non riescono a modificare, nei tempi richiesti dal mercato, i propri processi, le strutture organizzative nate e cresciute (e finanziate) in una logica di silos, le proprie competenze. E il rischio di non riuscire a rendere agile la propria capacità di risposta in un mercato dinamico come quello attuale (da considerare, tra le altre cose, gli impatti futuri legati a temi quali la sostenibilità aziendale e la transizione ecologica) espone l'azienda al pericolo di perdere competitività quando non peggio.

Quali prospettive per l'open innovation

Vedere la direzione futura di un fenomeno così complesso è arduo. Tuttavia è chiaro il punto discriminante tra successo e insuccesso: è legato alla tenacia di voler andare fino in fondo nella costruzione di un modello di open innovation che assicuri la partecipazione attiva, fin dall'inizio del processo, dei business team; dove i partner esterni che concorrono all'innovazione aziendale siano considerati, con processi, tecnologie, metriche di controllo e cultura "open", parte attiva e integrata dell'azienda e non solo soggetti esterni, semplici contributori di fatturato e realtà sperimentali. Serve anche poter misurare con maggiore certezza, attraverso Kpi aggiornati di continuo, l'impatto e l'efficacia delle strategie di open innovation per supportare in modo corretto le scelte strategiche aziendali. Ma è ormai un dato di fatto che la continua realizzazione di servizi e prodotti innovativi non possa più da tempo prescindere da competenze presenti in una galassia di partnership che l'azienda deve essere in grado di sviluppare e di curare.

GLI EDITORIALI DI BIZZIT

Innovazione: la tenacia, prima di tutto

CONTINUA A LEGGERE

GLI OSTACOLI DA SUPERARE

Sulla base di un'analisi degli errori ricorrenti commessi dalle aziende, la gran parte, che non sono riuscite ad attuare una piena open innovation (progetti non conclusi, scarso impatto sui fatturati, e così via), il gruppo del Politecnico ha messo a punto un toolkit operativo con un insieme di azioni da implementare basate sulle best practice e sugli errori raccolti durante le interviste e i casi studio. Ecco allora alcuni tra gli elementi utili da considerare:

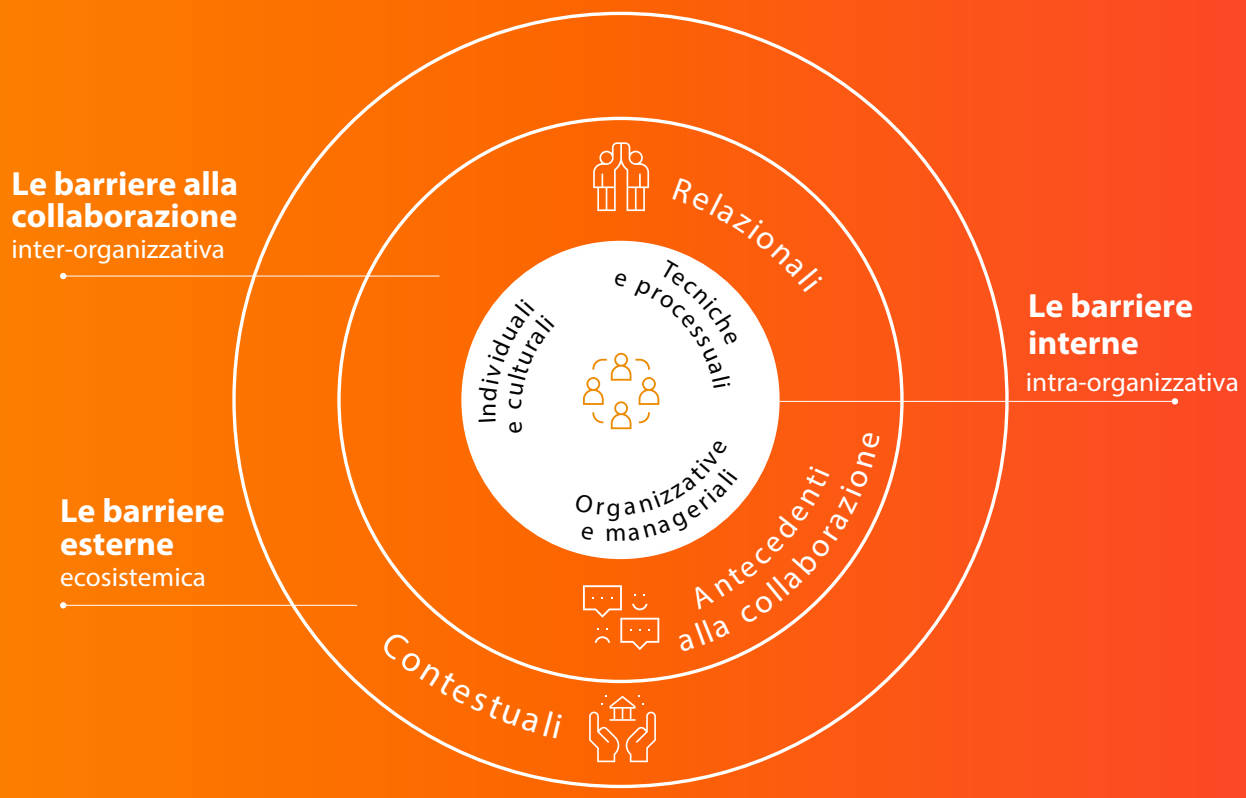
- Serve costruire un proprio approccio all'open innovation in modo che possa **riflettere l'identità aziendale** e rispondere così efficacemente alle esigenze di innovazione interne.
- La resistenza al cambiamento non è solo un freno culturale ma spesso dipende dalla **mancanza di comunicazione efficace** che riduce il flusso di idee innovative e limita il potenziale delle collaborazioni aziendali.
- La trasformazione dei confini tradizionalmente chiusi dell'organizzazione in modelli flessibili e permeabili alle innovazioni esterne determina un impatto ampio sull'azienda e deve **condizionare e coinvolgere ogni area, unità organizzativa, livello gerarchico.** Serve stabilire processi di cambiamento strutturati.
- Vanno identificate alcune **risorse chiave, persone e team focalizzati nella ricerca di soluzioni esterne** e in grado di guidare un processo di integrazione in azienda. Devono essere messi a punto **processi per selezionare e assimilare idee innovative nonché definite strutture** per supportare il coordinamento e l'apprendimento organizzativo.
- Bisogna diffondere nell'impresa un mindset aperto all'innovazione. La scusa al rifiuto del cambiamento si nasconde spesso dietro ostacoli organizzativi, facilmente ridefinibili. Si tratta di lavorare su tre diversi livelli di barriere: **culturali e individuali** (resistenze al nuovo, mancanza di una mentalità orientata all'innovazione e di fiducia nei confronti di nuove idee); **organizzative e manageriali** (rigidità delle strutture gerarchiche; mancanza di supporto da parte del top management da cui deriva una cultura aziendale poco favorevole all'innovazione); **tecniche e processuali** (adozione di nuove piattaforme tecnologiche e talvolta ridisegno parziale delle architetture informative e applicative per favorire la trasversalità dei contenuti e delle informazioni; accanto a questo vanno ripensati in parte, sempre nel com-

parto tecnologico, i processi e le tecnologie non allineati a un approccio di open innovation).

- La scelta dei partner e le modalità di interazione sono fondamentali. **La portata e la profondità di queste collaborazioni influenzano molto la capacità innovativa di un'impresa;** serve creare un ambiente di lavoro condiviso, con meccanismi e tecnologie efficaci di comunicazione, coordinamento e di accordo tra le parti.
- Vanno rimossi comportamenti opportunistici, disallineamenti sugli obiettivi e differenze culturali. Inoltre, la **mancanza di ruoli e responsabilità chiari nonché di processi operativi dedicati e formalizzati può compromettere il successo di una collaborazione.** Serve curare l'ecosistema delle relazioni con azioni di condivisione e coinvolgimento su regole e standard comuni.
- Vanno ricercate **competenze specialistiche nell'area dell'innovazione organizzativa e competenze nell'area contrattuale e della compliance** per supportare la gestione degli aspetti burocratici nelle partnership. Serve anche evitare un'eccessiva complessità e livello di dettaglio nella definizione dei contratti legali per favorire flessibilità nella gestione della collaborazione.

FRAME PER LA CLASSIFICAZIONE DELLE BARRIERE ALL'OPEN INNOVATION

Fonte: "Italian Open Innovation Lookout 2024" - Politecnico di Milano



Ransomware: un'evoluzione costante che sfida le difese informatiche

Le tattiche utilizzate dai cybercriminali per eseguire attacchi ransomware e ottenere il riscatto continuano ad adattarsi e raffinarsi per sfuggire alla crescente efficacia delle difese informatiche. Scopriamo i nuovi trend.

di **Riccardo Florio**

Nel panorama della sicurezza informatica, il ransomware rappresenta una delle minacce più insidiose e in continua evoluzione. Nonostante i progressi significativi nel campo delle difese informatiche, i cybercriminali affinano costantemente le loro tecniche, dimostrando una capacità di adattamento che complica enormemente il compito di chi si occupa di proteggere i dati sensibili.

Ogni anno emergono nuove varianti di ransomware, più sofisticate e difficili da rilevare, che sfruttano vulnerabilità inaspettate e adottano tattiche sempre più ingegnose per penetrare nei sistemi aziendali e personali.

In questo contesto, comprendere i trend emergenti diventa essenziale per anticipare le mosse degli attaccanti e rafforzare le difese contro un nemico che non cessa di reinventarsi. L'implementazione di un monitoraggio continuo, l'adozione di tecniche di rilevamento basate sul comportamento, e la preparazione per rispon-

dere agli attacchi anche al di fuori degli orari lavorativi standard sono diventate necessità imprescindibili per mitigare i rischi di attacchi ransomware moderni.

Le tecniche Living off the Land (LOTL)

Una delle principali tattiche emergenti è l'uso delle tecniche Living off the Land (LOTL). Questo approccio prevede **l'utilizzo di strumenti e funzionalità già presenti nei sistemi operativi e nei software legittimi** per portare a termine gli attacchi, evitando l'uso di malware esterni che potrebbero essere rilevati da software antivirus e altre difese. Per esempio, i criminali informatici possono sfruttare script di amministrazione di sistema o strumenti di gestione remota che sono già installati sui dispositivi bersaglio.

L'uso di questi strumenti legittimi rende molto più difficile rilevare l'attacco perché l'attività sembra normale agli occhi delle soluzioni di sicurezza. La crescente adozione di queste tecniche rende le difese tradizionali, come il rilevamento basato su firme, meno efficaci, spingendo le aziende a investire in soluzioni di sicurezza più avanzate, come l'analisi comportamentale e l'Endpoint Detection and Response (EDR).

Attacchi notturni

Un altro cambiamento significativo è il timing degli attacchi ransomware. I criminali hanno iniziato a concentrare le loro attività **nelle ore notturne, in particolare tra l'1 e le 5 del mattino**, quando il personale IT è meno presente o attivo. Questo lasso di tempo permette agli aggressori di sfruttare la minore vigilanza delle organizzazioni, con minori probabilità che un attacco venga individuato e bloccato rapidamente. Questo cambiamento nella tempistica richiede che le aziende adottino soluzioni di monitoraggio continuo e risposte rapide agli incidenti, idealmente supportate da un Security Operations Center (SOC) attivo 24 ore su 24.

I tempi d'attacco diventano più rapidi

Un'altra tendenza preoccupante è l'accelerazione dei tempi di attacco. Tradizionalmente, gli attacchi ransomware potevano svolgersi nell'arco di settimane, con gli aggressori che si muovevano lentamente per penetrare la rete, esfiltrare dati e poi crittografare i sistemi.

Tuttavia, nel 2023 e nel 2024, il tempo necessario per completare un attacco è diminuito drasticamente, **passando da settimane a poche ore.** Questo significa che le organizzazioni hanno molto meno tempo per rilevare e rispondere a un attacco prima che i dati vengano compromessi. La rapidità di questi attacchi impone l'adozione di tecnologie di rilevamento e risposta che possano operare in tempo reale, riducendo al minimo il danno potenziale.

Diffusione geografica

Gli Stati Uniti rimangono il principale obiettivo degli attacchi ransomware a livello globale. Secondo Malwarebytes, il 48% di tutti gli attacchi ransomware ha avuto luogo negli Stati Uniti, evidenziando la vulnerabilità delle infrastrutture e delle aziende americane a questo tipo di minaccia. Questa predominanza può essere attribuita alla vasta digitalizzazione del paese, che offre un ampio bacino di potenziali vittime, dalle grandi imprese ai servizi essenziali.
Nel Regno Unito, la situazione è altrettanto preoccupante. Gli attacchi ransomware sono aumentati del 67% nel corso del 2023, superando persino la crescita osservata negli Stati Uniti.
Questo incremento indica una crescente attenzione dei cybercriminali verso il mercato britannico, probabilmente a causa della sua robusta economia digitale e delle numerose aziende di medie dimensioni che rappresentano bersagli lucrativi ma meno protetti.
Nel 2024, l'Italia continua a essere uno dei paesi europei maggiormente colpiti dagli attacchi ransomware, consolidando una posizione critica già osservata negli anni precedenti. Secondo i dati di **Cyberint** relativi al secondo trimestre 2024, dopo Stati Uniti e UK, i paesi più colpiti sono Canada e Germania con **l'Italia che si colloca al quinto posto.**

CYBERINT
Ransomware Groups Report 2024
Secondo quadrimestre

ACCEDI AL REPORT

I settori più colpiti

I cybercriminali stanno costantemente perfezionando le loro strategie per colpire settori critici e regioni con un alto tasso di digitalizzazione.
Alcuni settori sono particolarmente bersagliati dagli attacchi ransomware, con il **settore sanitario e quello dell'istruzione** che emergono come i più vulnerabili. Il 60% degli attacchi ransomware nel settore dell'istruzione e il 71% di quelli nel settore sanitario a livello globale sono avvenuti negli Stati Uniti. Questo è dovuto in parte alla criticità dei dati gestiti da questi settori, che rende i loro sistemi dei bersagli privilegiati per gli attaccanti che mirano a massimizzare i guadagni finanziari attraverso il riscatto.
Il settore **manifatturiero** ha visto un aumento significativo degli attacchi, con un incremento del 71% su base annua nel 2023. La digitalizzazione crescente e la natura spesso critica delle operazioni manifatturiere rendono questo settore particolarmente attraente per i criminali informatici. Le interruzioni nella produzione possono causare danni economici significativi, il che spinge le aziende a pagare rapidamente il riscatto per ripristinare le operazioni.

L'evoluzione nelle richieste di riscatto e nei pagamenti

Non solo le tecniche ma anche le modalità di pagamento e le strategia per masimizzare il guadagno evolvono.

Negli ultimi anni, il ransomware si è evoluto in modo significativo, non solo dal punto delle tecniche di attacco, ma anche nelle strategie e negli approcci che gli aggressori utilizzano per estorcere denaro alle loro vittime. Il rapporto "Sophos State of Ransomware 2024" evidenzia diverse tendenze chiave nelle modalità di organizzazione delle richieste e nei metodi utilizzati dagli aggressori per massimizzare i loro guadagni.

Cresce la richiesta del riscatto e i metodi per richiederlo

Una delle tendenze più evidenti è il drammatico **aumento dell'importo medio delle richieste di riscatto.** Secondo il rapporto, il pagamento medio del riscatto è passato da 812.380 dollari nel 2022 a oltre 1,5 milioni di dollari nel 2023. Questo forte aumento può essere attribuito a una serie di fattori, tra cui l'adozione di strategie indirizzate sempre più a colpire grandi organizzazioni con ampie disponibilità economiche.

SCARICA IL REPORT
Sophos State of Ransomware 2024

Questi aggressori spesso chiedono riscatti multimilionari, soprattutto quando sanno che le loro vittime, spesso operanti in settori critici come la sanità, il manifatturiero e l'istruzione, sono disposte a pagare somme elevate per evitare l'interruzione dei servizi e la perdita di dati sensibili.

Tipologia delle richieste e approccio alla negoziazione

Anche **i metodi utilizzati per richiedere e garantire i riscatti** si sono evoluti. Tradizionalmente, gli attacchi ransomware prevedevano la cifratura dei dati della vittima e la richiesta di un pagamento in cambio della chiave di decifrazione. Tuttavia, gli aggressori utilizzano sempre più spesso una doppia tattica di estorsione, in cui non solo cifrano i dati ma li copiano anche, minacciando di pubblicare o vendere le informazioni rubate se non viene pagato il riscatto.
Questa ulteriore pressione spesso costringe le vittime a pagare, poiché il rischio di far trapelare dati sensibili può essere ancora più dannoso della perdita di accesso a tali dati per i correlati danni reputazionali e legali.

A volte esiste anche un terzo livello di estorsione che si estende ai partner commerciali delle vittime. Gli attaccanti hanno affinato anche **l'approccio alle negoziazioni**, spesso iniziando con richieste esorbitanti, con l'aspettativa di negoziare verso il basso fino a mantenere, comunque, un importo significativo. In alcuni casi, i gruppi di ransomware impiegano negoziatori professionisti per gestire le discussioni, assicurandosi di massimizzare il guadagno finale. Il report di Sophos evidenzia che il 70% degli attacchi ransomware nel 2024 ha comportato la crittografia dei dati, ma solo una parte delle vittime ha pagato l'intero ammontare richiesto inizialmente, con la maggior parte delle trattative che portano a un pagamento inferiore, seppur significativo.

Metodi di pagamento e il ruolo delle criptovalute

Le criptovalute continuano ad essere il metodo di pagamento preferito per le richieste di riscatto, grazie al loro anonimato e alla difficoltà di tracciamento. Tuttavia, con le autorità sempre più efficaci nel tracciare le transazioni in criptovalute, **alcuni cybercriminali stanno esplorando alternative**, come criptovalute meno conosciute o addirittura metodi di pagamento frammentati in più transazioni per ridurre la possibilità di rintraccio.

In alcuni casi, i gruppi ransomware hanno persino iniziato a offrire piani di pagamento rateizzati, permettendo alle vittime di dilazionare il riscatto su più tranche. Questa tattica non solo aumenta la probabilità di pagamento, ma permette agli attaccanti di mantenere il controllo sulla vittima per un periodo di tempo più lungo, riuscendo potenzialmente a estorcere più denaro nel lungo periodo.

SCARICA IL REPORT *sui Crimini nel Mondo delle Criptovalute 2024, con le ultime tendenze in ransomware, truffe e hacking.*

Il riscatto si paga spesso

Il metodo più sicuro ed efficace per recuperare i dati dopo un attacco ransomware è certamente l'uso di backup regolari e aggiornati effettuati da "vault" mantenuti sicuri. Le organizzazioni che mantengono backup offline o separati dalla rete principale sono in grado di ripristinare i loro dati senza dover cedere alle richieste degli attaccanti. Il backup riduce il rischio di perdita permanente di dati e limita il tempo di inattività, permettendo alle aziende di riprendere rapidamente le operazioni normali.

Tuttavia, il successo del ripristino dipende dalla frequenza e dalla qualità dei backup, nonché dalla loro protezione contro gli attacchi stessi, che talvolta prendono di mira i backup per renderli inutilizzabili.

Il report di Sophos evidenzia che, nonostante le raccomandazioni

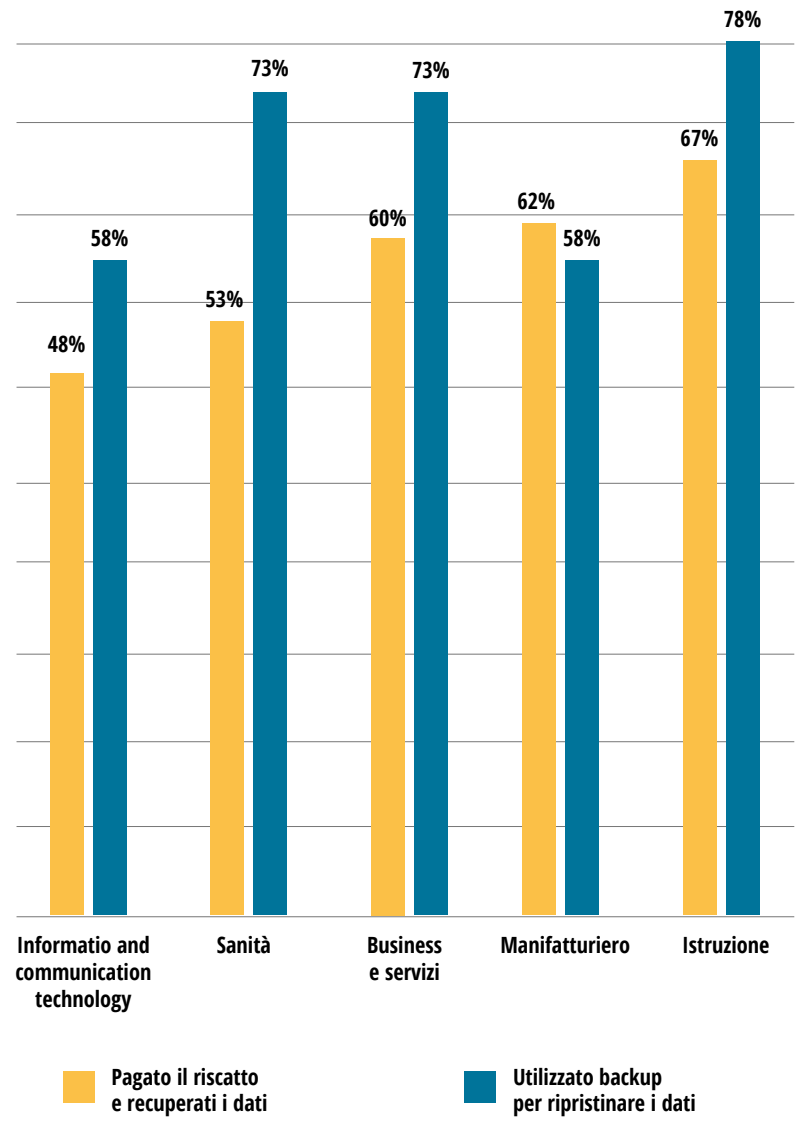
contrarie degli esperti di sicurezza, **molte organizzazioni decidono di pagare il riscatto** richiesto dai cybercriminali per riottenere l'accesso ai propri dati.
Tuttavia, questa pratica è rischiosa e spesso controproducente. Anche dopo il pagamento, non c'è garanzia che gli attaccanti forniscano le chiavi di decrittazione o che i dati recuperati siano completi e non danneggiati. Inoltre, in molti casi chi paga il riscatto torna a essere spesso vittima del ransomware, anche da parte della medesima organizzazione criminale.

Variazioni per settore e approcci alla restituzione dei dati

Le strategie per il recupero dei dati variano notevolmente in base al settore e alla criticità delle operazioni aziendali. Mentre alcune organizzazioni scelgono di pagare il riscatto per velocizzare il ripristino, altre preferiscono investire in backup robusti e nella resilienza dei sistemi per evitare di dover trattare con i criminali. L'impatto del ransomware varia, dunque, significativamente da settore a settore.
La **sanità**, per esempio, si dimostra particolarmente vulnerabile, poiché le ripercussioni in questo settore possono essere particolarmente gravi, non solo per l'interruzione dei servizi essenziali, ma anche per il rischio di esposizione di dati sensibili dei pazienti. Un altro esempio significativo è dato dalle aziende del settore **manifatturiero** che sono fortemente dipendenti da processi digitali e automazione, trovandosi di fronte a un rischio elevato di interruzioni operative e di ingenti perdite finanziarie se non riescono a ripristinare rapidamente i loro sistemi.

Metodi di recupero dati per settore
La frequenza con cui i dati vengono recuperati utilizzando i backup e pagando il riscatto

Fonte: Sophos Whitepaper - Aprile 2024



SOPHOS
The State of Ransomware 2024

ACCEDI AL REPORT INTEGRALE

GLI APPROFONDIMENTI DI BIZZIT

RANSOMWARE E AI GENERATIVA

L'intelligenza artificiale generativa sta rivoluzionando il panorama del ransomware, rendendo gli attacchi più sofisticati e difficili da rilevare. Grazie alle sue capacità, gli hacker possono personalizzare attacchi di phishing su vasta scala, creando email, messaggi o post sui social media che imitano perfettamente il tono e lo stile di fonti affidabili, aumentando così le probabilità che le vittime clicchino su link dannosi o scarichino file infetti.
Inoltre, l'AI generativa permette di ottimizzare i payload del ransomware. Algoritmi avanzati possono analizzare dati rubati o pubblici per individuare file critici di un'organizzazione, criptando selettivamente quelli più preziosi per massimizzare l'impatto e incentivare il pagamento del riscatto.
La capacità di adattamento continuo dell'AI è particolarmente preoccupante: può testare e modificare i payload fino a superare le difese di sicurezza, creando un ciclo costante di evoluzione delle minacce. Questo rende le contromisure più difficili da mantenere efficaci nel lungo termine.

continua a leggere

Il futuro

In prospettiva, le tendenze identificate suggeriscono che il ransomware continuerà a evolversi, con gli aggressori che probabilmente svilupperanno metodi ancora più sofisticati per estorcere denaro alle loro vittime.
Mentre le organizzazioni migliorano le loro difese e le forze dell'ordine diventano più efficaci nell'interrompere le operazioni di ransomware, gli aggressori si concentreranno probabilmente sull'affinamento delle loro richieste e delle tattiche di negoziazione per massimizzare i loro profitti e minimizzare il rischio di essere scoperti.
Inoltre, si prevede che l'uso dell'intelligenza artificiale possa giocare un ruolo chiave nel perfezionare questi attacchi.
Per le aziende, questo significa che le misure di cybersecurity sono più importanti che mai. Le aziende devono non solo proteggere i propri dati dalla crittografia, ma anche prepararsi alla possibilità di attacchi con multipla estorsione e alle complesse negoziazioni che possono seguire a un incidente ransomware. Tenendosi informate sulle ultime tendenze e sulle tattiche in evoluzione, le organizzazioni possono posizionarsi meglio per difendersi da queste minacce sempre più sofisticate.

Sicurezza: questione di piattaforma

di **Fabrizio Pincelli**

Nell'annuale appuntamento con partner, clienti e prospect italiani, SentinelOne delinea le strategie inerenti alla Singularity Platform e anticipa la roadmap della sua proposta Purple AI

"Oggi la sicurezza non è più soltanto un costo, è un abilitatore del business. Fornisce un aiuto essenziale alle organizzazioni a essere produttive, a non subire momenti di stop operando in maniera protetta e sicura". Così si è espresso **Paolo Cecchi, sales director per la Mediterranean Region di SentinelOne**, aprendo i lavori dell'annuale incontro con partner, clienti e prospect italiani. Siccome, però, le minacce sono sempre più sofisticate ed efficaci bisogna sapersi difendere in modo adeguato. Una sfida che, secondo Cecchi, ha portato i responsabili della sicurezza a concentrarsi su tre principali obiettivi. Il primo è di cercare di **mitigare il rischio**, sia per ridurre la possibilità di essere vittima di attacchi sia per limitare le eventuali conseguenze qualora un attacco raggiungesse i suoi scopi.
Il secondo obiettivo è **semplificare le Operation.** *"In molti Paesi europei* - spiega Cecchi - *ci sono aziende che, in virtù delle loro dimensioni, si possono permettere investimenti importanti in sicurezza,*

se non addirittura di avere un SOC interno con persone dedicate. In Italia, invece, la prevalente presenza di PMI porta a investimenti più contenuti. Perciò, diventa cruciale per le imprese poter semplificare le Operation attraverso una piattaforma unificata, basata su strumenti di intelligenza artificiale e automazione".
Il terzo obiettivo è il **contenimento dei costi.** "Do more with less" è la richiesta che tutti ricevono quotidianamente. Di nuovo, *"un approccio basato su una piattaforma unificata permette di offrire un'efficace risposta a tale richiesta, consentendo sia di non disperdere risorse in termini di persone e tecnologie sia di ottimizzare i processi"*.

Un'evoluzione che complica la sicurezza

D'altro canto, la trasformazione digitale ha creato un inevitabile problema legato alla gestione dei dati. Quotidianamente se ne produce un'enorme quantità e ogni dato può diventare un valido appiglio per un attaccante potendo, quindi, essere sottratto e utilizzato per remunerativi scopi illeciti. Non dimentichiamo, infatti, che **oltre l'83% degli attacchi globali ha come obiettivo l'estorsione di denaro**, secondo quanto riportato dal Rapporto Clusit 2024.
Diventa perciò strategico **avere una visibilità "real time" sui dati** ma, considerata la loro numerosità, se non si usa l'automazione non si riesce ad avere un efficace controllo su tali dati. A complicare le cose contribuisce poi il sempre più diffuso ricorso al cloud. Con l'adozione di soluzioni cloud native, le reti aziendali non sono più limitate da confini definiti come accade con l'on-premise, ma si espandono incrementando la superficie di attacco. E questo rende sempre più difficile mantenere una chiara visibilità sull'infrastruttura aziendale. *"Quando si parla di allestire un sistema di protezione, oggi non ci si può più limitare a proteggere un singolo endpoint, un server o un asset all'interno di un'organizzazione* – osserva **Paolo Ardemagni, vice president Southern EMEA di SentinelOne** -. *Si deve disporre di una soluzione che consenta una protezione globale sia sui dati sia sull'infrastruttura, che operi in tempo reale e che sia facile da gestire"*. SentinelOne risponde a tali esigenze attraverso la sua **Singularity Platform**. *"Nasciamo come società per la protezione dell'endpoint, ma non basta più per avere un elevato grado di sicurezza in azienda* - prosegue Ardemagni -. *Oggi* ***forniamo una piattaforma, perché è l'unico modo per proteggere adeguatamente un'azienda*****.** *In tal senso, Singularity Platform permette l'ingestion di dati provenienti anche da soluzioni di sicurezza esterne. Abbiamo un marketplace dove poter selezionare le sorgenti e integrarle in*

Paolo Ardemagni, vice president Southern EMEA di SentinelOne

maniera estremamente semplice. E se il connettore non è presente è possibile crearne uno ad hoc attraverso le interfacce API". La piattaforma è potenziata dall'**intelligenza artificiale, che in casa SentinelOne prende il nome di Purple AI**, e sopra tale piattaforma si possono innestare molteplici soluzioni, capaci di spaziare dalla protezione dell'endpoint a quella di dati e applicazioni in cloud, dalla protezione dell'entità all'exposure management. Nel caso ve ne fosse la necessità, sono anche disponibili servizi gestiti di detection e response. *"Anzi di managed extended detection e response (MXDR) perché arriverà a breve un servizio che non solo permetterà di gestire la telemetria dei nostri sistemi di protezione degli endpoint ma anche quella delle soluzioni esterne"*.

Un aiuto agli analisti

Purple AI è disponibile sul mercato dall'inizio di aprile 2024 ed è l'ultima evoluzione della ricerca in tema di intelligenza artificiale che ha caratterizzato SentinelOne negli ultimi 10 anni. *"Purple AI non è pensata per aiutare gli utenti, perché sono già difesi dall'agent SentinelOne, quanto invece per potenziare la figura dell'analista* - precisa **Marco Rottigni, technical director di SentinelOne** -. *È uno strumento dedicato alle Security Operations e ha l'obiettivo di fornire una notevole accelerazione delle investigazioni, del threat hunting e della trasformazione di telemetria grezza in informazioni"*.
Rottigni ha inoltre evidenziato che i dati processati da Purple AI restano di esclusiva pertinenza dell'azienda che utilizza quella determinata istanza dell'intelligenza artificiale. *"Si tratta di un modello GPT (Generative Pre-trained Transformer) che, quindi, interagisce con gli analisti, ma l'interazione rimane all'interno della "subscription" che è mantenuta nell'area geografica scelta dal cliente. L'architettura di Purple AI è basata su un agente, un orchestratore che SentinelOne ha chiamato Asimov e su un'architettura RAG con modelli LLM"*.

La roadmap di Purple AI

Purple AI è la più recente evoluzione della ricerca di SentinelOne in ambito intelligenza artificiale, ma non è l'ultima. Infatti, all'orizzonte si profilano già importanti novità. Tra quelle più di rilievo, citiamo **Purple AI for Alert Summaries** che dovrebbe arrivare entro l'estate: permetterà all'intelligenza artificiale di fare un resoconto di quanto successo in un incidente e di eseguire le opportune verifiche.
Più avanti vedremo altre evoluzioni importanti quali **Purple AI for Auto Triage**, che permetterà a Purple AI di fornire un primo triage delle informazioni di un incidente informatico, facilitando ed accelerando l'efficienza operativa degli analisti.
Altra novità evolutiva importante è sicuramente **Purple AI for Investigation**: si userà l'intelligenza artificiale non solo per identificare anomalie ma anche per proporre in automatico procedure di risposta. Il tutto in modalità no code, quindi alla portata di tutti.

L'APPROFONDIMENTO

Cyber security, SentinelOne va verso la totale automazione

continua a leggere

L'identità governata

di **Riccardo Florio**

Grazie a funzionalità avanzate di automazione, intelligenza artificiale e integrazione con altri sistemi di sicurezza, le soluzioni NetIQ di OpenText per l'amministrazione e la governance dell'identità garantiscono la compliance e forniscono una protezione efficace contro minacce come il ransomware

Pierpaolo Alì
director Southern Europe
di OpenText Cybersecurity

Con la trasformazione digitale, **cresce la complessità** dovuta all'aumento dei servizi e alla loro distribuzione geografica, al rafforzamento dei requisiti di conformità e all'esigenza di gestire i rischi e applicare i principi di sicurezza del privilegio minimo.

Sebbene l'automazione resti un pilastro fondamentale per la gestione delle identità è sempre più indispensabile allineare i processi operativi a politiche di governance che garantiscano una visibilità completa e una gestione efficace dei privilegi.

Le **soluzioni OpenText per l'identity governance and administration** coniugano gestione dell'identità e governance dell'accesso per gestire i rischi in modo centralizzato. Tra queste, NetIQ Identity Manager, NetIQ Access Manager e NetIQ Identity Governance sono tre strumenti chiave, capaci di operare

in modo indipendente ma di integrarsi tra loro per garantire una gestione completa delle identità e degli accessi.
Le differenze tra questi strumenti risiedono principalmente nel loro **scopo e ambito d'azione ma anche nell'approccio all'automazione e alla governance**.

NetIQ Identity Manager: gestione centralizzata delle identità

NetIQ Identity Manager rappresenta una delle soluzioni più consolidate e avanzate per la gestione delle identità. Si concentra sull'**automazione del ciclo di vita delle identità digitali degli utenti all'interno di un'organizzazione**, con l'obiettivo di garantire che ogni dipendente, collaboratore o sistema disponga dei permessi appropriati per accedere alle risorse aziendali. Il suo punto di forza è la capacità di automatizzare il provisioning e il deprovisioning degli utenti, riducendo gli errori umani e migliorando l'efficienza operativa in ambienti caratterizzati da grandi quantità di account e applicazioni.
Tra le sue principali caratteristiche troviamo l'integrazione con diverse piattaforme e la possibilità di monitorare in tempo reale gli accessi, fornendo una visione centralizzata e granulare su chi accede a cosa all'interno dell'organizzazione, indipendentemente dal numero di applicazioni e sistemi in uso.
L'evoluzione di questa piattaforma negli ultimi anni ha visto l'integrazione di tecnologie basate sull'intelligenza artificiale, che permettono di analizzare i comportamenti degli utenti e identificare eventuali anomalie in tempo reale.

NetIQ Access Manager: controllo dell'accesso contestuale e Single Sign-On (SSO)

NetIQ Access Manager si occupa principalmente di **gestire gli accessi mobili e Web fornendo un'autenticazione centralizzata e controllo automatizzato degli accessi** basato sul contesto. Questa soluzione è ideale per proteggere le applicazioni Web e migliorare l'esperienza dell'utente semplificando l'accesso a più sistemi tramite una singola autenticazione. La sua funzione più conosciuta è, infatti, il **Single Sign-On (SSO)**, che consente agli utenti di accedere a più applicazioni con un'unica autenticazione, semplificando l'esperienza utente e migliorando la sicurezza. Il sistema permette, inoltre, di creare politiche di accesso basate su criteri personalizzati quali, per esempio, il dispositivo utilizzato, la posizione geografica o l'orario dell'accesso. Questo rende Access Manager particolarmente utile in scenari in cui è necessaria una gestione dinamica degli accessi, soprattut-

to per proteggere le applicazioni aziendali accessibili da remoto o su dispositivi non aziendali.

NetIQ Identity Governance: governance e conformità delle identità

NetIQ Identity Governance è la soluzione che completa questa triade, focalizzandosi sulla governance e la conformità degli accessi. Mentre Identity Manager si occupa di automatizzare la gestione delle identità, Identity Governance garantisce che tali **accessi siano continuamente monitorati e verificati per essere conformi alle normative aziendali e legali** e assicurando che siano concessi solo a chi ne ha realmente bisogno, bloccando gli accessi non autorizzati, che rappresentano una delle principali cause di violazione dei dati. La governance delle identità è cruciale in un'era in cui le organizzazioni devono rispettare normative severe, come il GDPR o il SOX, che richiedono audit regolari e verifiche continue sui diritti di accesso. Questo strumento permette alle aziende di monitorare costantemente l'utilizzo delle identità, **abilitando audit continui dei diritti di accesso degli utenti**, assicurando che gli accessi siano giustificati e costantemente conformi alle normative sulla privacy e sulla sicurezza dei dati. Inoltre, grazie alla sua capacità di audit, permette di mantenere una tracciabilità completa e di identificare eventuali discrepanze o accessi non autorizzati.

GOVERNARE L'IDENTITÀ PROTEGGE DAL RANSOMWARE

Le soluzioni di gestione e governance delle identità di OpenText offrono un'efficace protezione contro le minacce, automatizzando la gestione degli accessi e monitorando continuamente i comportamenti degli utenti.

Grazie a questo monitoraggio costante, è possibile rilevare tempestivamente attività sospette che potrebbero essere legate a un attacco ransomware, il quale spesso si basa sull'ottenimento di accessi privilegiati per infiltrarsi nella rete aziendale.

Un ulteriore elemento chiave delle soluzioni OpenText nel contrasto al ransomware è la loro capacità di sfruttare le tecnologie integrate di machine learning per identificare e bloccare comportamenti anomali prima che possano causare danni significativi, rispondendo proattivamente alle minacce. In aggiunta, NetIQ Identity Manager supporta la segmentazione degli accessi, riducendo così il potenziale impatto di un attacco su larga scala e limitando la diffusione di eventuali minacce all'interno dell'infrastruttura aziendale.

Per conoscere le soluzioni di OpenText Cybersecurity CLICCA QUI

Un approccio unificato per prevenire ogni minaccia

di **Riccardo Florio**

WithSecure fornisce una soluzione integrata e proattiva per proteggere le aziende dalle minacce cyber, grazie a strumenti avanzati di gestione delle esposizioni, rilevamento e risposta basati sull'intelligenza artificiale.

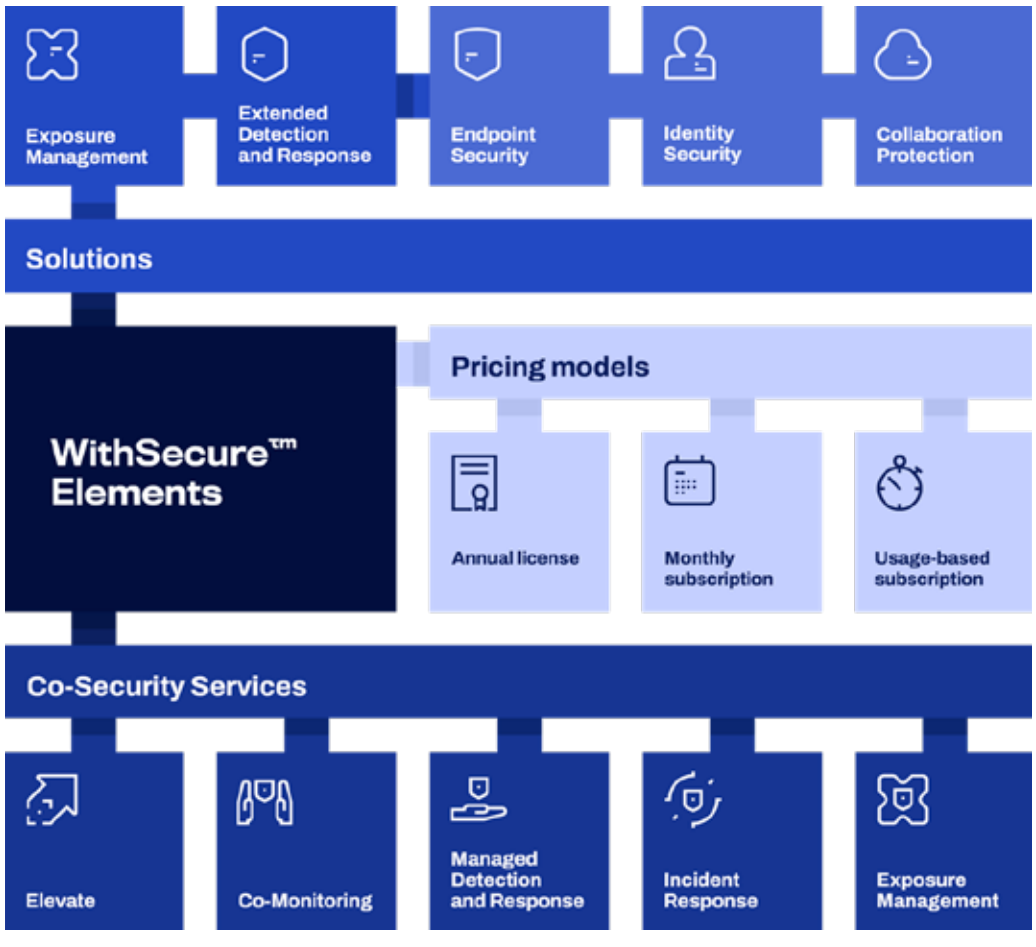
Nell'era digitale odierna, le aziende operano in ambienti sempre più complessi e frammentati, spesso caratterizzati da infrastrutture ibride che combinano risorse locali, cloud pubblici e privati, dispositivi mobili e reti remote. Questa trasformazione ha reso i confini tra i sistemi aziendali e l'esterno sempre più sfumati, aumentando, di conseguenza, la superficie di attacco.

La sfida **non riguarda più soltanto la protezione dei dati sensibili e dei sistemi aziendali, ma anche la salvaguardia della continuità operativa** contro minacce provenienti dall'esterno come dall'interno. Per identificare, monitorare e neutralizzare i possibili percorsi d'attacco verso le risorse critiche serve una visione completa e integrata, capace di coprire l'intero spettro delle potenziali vulnerabilità nonché di fornire una risposta rapida ed efficiente.

Una piattaforma di sicurezza modulare e integrata

Per rispondere a queste nuove esigenze di sicurezza, WithSecure ha sviluppato la **WithSecure Elements Platform**, una piattaforma di sicurezza informatica modulare che combina molteplici funzionalità chiave come il **rilevamento e la risposta estesa (XDR), la gestione dell'esposizione (XM) e i servizi di co-sicurezza.**

Queste componenti, integrate in un'unica interfaccia centralizzata, permettono di proteggere l'intera infrastruttura aziendale da una vasta gamma di minacce, tra cui ransomware, malware, attacchi persistenti avanzati (APT) e molto altro, favorendo un'evoluzione della sicurezza da un approccio reattivo a uno proattivo.



Attraverso il **WithSecure Elements Security Center** è, infatti, possibile ottenere una visione d'insieme in tempo reale dello stato di sicurezza di utenti e dispositivi, permettendo agli operatori di identificare le minacce e intervenire tempestivamente con strumenti di remediation semplici ed efficaci.

Bloccare gli attacchi che sfruttano l'identità

Con l'aumento del lavoro da remoto e l'adozione di applicazioni cloud, le identità digitali sono diventate il nuovo bersaglio privilegiato del cyber crimine. Uno degli aspetti più critici nell'attuale scenario della cybersecurity è proprio la possibilità che un attaccante riesca a sfruttare un'identità compromessa per ottenere accesso a dati e risorse in modo considerato legittimo dalla maggior parte dei sistemi di protezione. Questi attacchi solitamente partono da un accesso apparentemente innocuo, come una email aziendale, per estendersi poi a diverse applicazioni critiche, inclusi i sistemi di gestione aziendale, i database e i servizi cloud, rischiando di rimanere al lungo inosservati.

Per queste esigenze, **WithSecure Elements XDR**

ha predisposto Elements Identity Security, che sfrutta la tecnologia Microsoft Entra ID (in precedenza conosciuto come Azure Active Directory) per proteggere chi opera da remoto e le applicazioni aziendali basate su cloud da attacchi rivolti alla compromissione dell'identità.

Elements Identity Security lavora in modo integrato con il resto della piattaforma WithSecure Elements, fornendo: visibilità completa su tutte le identità digitali, strumenti di autenticazione multi-fattore (MFA), gestione degli accessi condizionali e monitoraggio in tempo reale su chi accede alle risorse aziendali e da dove.

Una delle caratteristiche più interessanti di Elements Identity Security è la sua capacità di agire come **una sorta di "sistema di allarme" in tempo reale per le identità digitali,** costantemente alla ricerca di comportamenti fuori dall'ordinario, come tentativi di accesso da località insolite, cambiamenti improvvisi nei pattern di utilizzo o tentativi di bypassare i protocolli di sicurezza.

Quando viene rilevata una potenziale minaccia, la piattaforma invia immediatamente notifiche agli amministratori di sistema, suggerendo azioni correttive da intraprendere per neutralizzarla.

Prevenire gestendo il livello di esposizione

In un panorama digitale in costante evoluzione, la protezione delle informazioni sensibili e delle infrastrutture critiche richiede un approccio proattivo che **non si limiti a reagire alle minacce, ma che sia in grado di prevederle e prevenirle.** Le tecnologie di "exposure management" si collocano proprio in questo ambito, offrendo strumenti per identificare, valutare e affrontare continuamente le vulnerabilità presenti nelle risorse digitali di un'organizzazione.

L'obiettivo è quello di ridurre al minimo le possibilità di attacco, identificando proattivamente i punti deboli nei sistemi aziendali, sia all'interno sia all'esterno.

Come afferma **Carmen Palumbo, country sales manager Italia di WithSecure**, *"L'adozione di una soluzione per la gestione costante del livello di esposizione fornisce una vi-*

Carmen Palumbo,
country sales manager
Italia di WithSecure

sione completa del rischio aziendale. Attraverso strumenti come scanner di vulnerabilità, feed di threat intelligence e simulazioni di attacco, le aziende possono valutare il rischio in tempo reale e applicare rapidamente le contromisure necessarie per mitigarlo, minimizzando così l'esposizione alle minacce".

WithSecure Elements Exposure Management

Per affrontare le sfide della gestione delle esposizioni, WithSecure ha sviluppato **Elements Exposure Management (XM)**, una piattaforma avanzata e basata sull'intelligenza artificiale che **offre una vista unificata delle esposizioni digitali più critiche, simulando percorsi di attacco e suggerendo le azioni più efficaci** per rafforzare le difese.

Grazie alla potenza dell'AI, questa soluzione è in grado di analizzare in modo continuo la superficie di attacco dell'azienda e correlarla alla postura di sicurezza interna, prevedendo i possibili punti deboli e fornendo raccomandazioni personalizzate per prevenire potenziali violazioni.

"Elements XM - precisa **Andrea Muzzi, technical manager di WithSecure** - *combina i dati provenienti dalla superficie di attacco esterna, dai sistemi di gestione delle identità (come Microsoft Entra ID), dai dispositivi, dalla rete e dai servizi cloud (Azure, AWS). La soluzione arricchisce questi dati con informazioni in tempo reale sulle minacce e sul contesto aziendale per un approccio olistico alla sicurezza. Le raccomandazioni basate sull'AI includono indicazioni per i team tecnici su come intraprendere rapidamente le azioni più impattanti e rendono i rischi per la sicurezza facilmente comprensibili per i decisori aziendali".*

Un approccio proattivo per fronteggiare gli attacchi ransomware

Un ulteriore punto di forza della piattaforma WithSecure Elements è la **sua capacità di prevenire attacchi ransomware.**

Grazie all'utilizzo dell'AI e di strumenti avanzati di analisi delle esposizioni, le aziende possono **individuare e correggere i punti deboli prima che vengano sfruttati dai criminali informatici** e prevenire violazioni.

Andrea Muzzi, technical manager di WithSecure

"La dashboard di Elements - spiega Palumbo – *fornisce in tempo reale una visione unificata e intuitiva della superficie d'attacco, delle risorse critiche a rischio e dei passaggi praticabili per eliminare i punti deboli che gli attaccanti amano sfruttare. Inoltre, il nostro motore di raccomandazioni alimentato dall'intelligenza artificiale agisce come un team di analisti virtuali che lavora 24 ore su 24 per individuare e bloccare possibili percorsi d'attacco. I team di sicurezza possono così monitorare la situazione , individuare le vulnerabilità più pericolose e prendere decisioni informate per la protezione delle risorse aziendali".*

I servizi di co-sicurezza: una collaborazione strategica

WithSecure Elements è una soluzione, **progettata specificamente per le aziende di medie dimensioni che necessitano di soluzioni di sicurezza robuste e scalabili e per i loro partner di servizi di sicurezza,** utilizzabile attraverso una gestione interna sul WithSecure Elements Cloud oppure tramite un service provider, partner di WithSecure.

Il rapporto con i partner è un elemento distintivo della strategia di WithSecure che promuove un modello di co-security con la stretta collaborazione tra l'azienda, i suoi partner di servizi IT e i clienti per fronteggiare insieme le sfide della sicurezza informatica.

"In WithSecure – conclude Palumbo - *co-security non è solo un concetto, ma un principio guida. Significa condividere tecnologie e risorse, rafforzare le capacità, le competenze e la cultura della sicurezza attraverso la partnership comprendendo che nessuna entità può affrontare da sola tutte le sfide della cybersecurity. Per questo motivo, WithSecure, i suoi partner di servizi IT e i suoi clienti lavorano insieme per garantire una protezione solida e completa. Insieme, formiamo un fronte unito contro le minacce, dando priorità alla capacità di preparazione, alla rapidità di risposta e all'adattabilità".*

Democratizzare la cybersecurity puntando al mid-market

Il ransomware colpisce in particolare le piccole e medie imprese, spesso prive delle risorse necessarie per difendersi in modo efficace, trovandosi così in difficoltà nel reperire soluzioni pratiche, accessibili e sostenibili.

WithSecure per risponde alle sfide di questo segmento mette a disposizione anche delle realtà più piccole gli strumenti necessari per disporre di un elevato livello di sicurezza a un costo accessibile e, soprattutto, con un livello di semplicità tale da non richiedere competenze che risultano tanto avanzate quanto difficili e costose da reperire.

PER SAPERNE DI PIÙ CLICCA QUI

Cybertech Europe 2024 pronto al via

Dal 8 al 9 ottobre, Roma ospiterà uno degli eventi più attesi nel mondo della cybersecurity.

a cura della **Redazione**

CybertechEurope, l'evento di riferimento per la cybersecurity in Italia, torna a **Roma l'8 e il 9 ottobre 2024 presso La Nuvola Convention Center**. L'edizione di quest'anno sarà ricca di contenuti, con numerosi espositori e una varietà di temi trattati. Rappresentanti delle istituzioni, del mondo industriale e dei principali vendor interverranno, e uno dei temi centrali sarà l'intelligenza artificiale, al centro di dibattiti sulle sue implicazioni nella sicurezza, seguendo il motto "AI for Cyber and Cyber for AI".
Si discuteranno i rischi legati all'AI, come deepfake, phishing e ransomware, così come le opportunità derivanti dalla sua integrazione nelle soluzioni di cybersecurity. Un focus speciale sarà dedicato alla capacità dell'AI di identificare proattivamente minacce, sia interne che esterne, con analisi avanzate in grado di rilevare pattern insoliti.
L'interconnessione tra **cyber resilienza e Operational Technology (OT)** sarà un altro tema di rilievo. La crescente apertura degli ambienti industriali verso il cloud ha cambiato radicalmente lo scenario rispetto al passato, quando le tecnologie OT erano isolate e più protette. Durante l'evento si terranno sessioni dedicate alla sicurezza del cloud, con un focus su soluzioni avanzate e difesa delle infrastrutture digitali.
Un altro tema cruciale sarà il ruolo della cybersecurity e della cyber defence nell'Unione Europea, con un approfondimento sulla guerra cibernetica e sui rischi per le infrastrutture critiche, in particolare attraverso la sessione "Multidomain critical infrastructures: from strategic assets to potential threats in a hybrid warfare scenario".
Si discuterà inoltre dei principi **Zero Trust e dei nuovi framework normativi** che stanno trasformando il panorama della cybersecurity, con un'attenzione speciale alla direttiva NIS2. Oltre alle sessioni principali, saranno organizzati workshop e stand per permettere ai partecipanti di interagire con le aziende e discutere le sfide della cybersecurity.

COME PARTECIPARE A CYBERTECH EUROPE 2024

In qualità di media sponsor, Reportec vi offre l'opportunità di ottenere un codice sconto del 20% sul biglietto di ingresso, utilizzando il codice **Paeur24rptc20**

REGISTRATI QUI INSERENDO IL CODICE Paeur24rptc20

Easynet e C.I.E. semplificano la digitalizzazione

di **Fabrizio Pincelli**

C.I.E. Telematica è diventata la sesta business unit di Easynet Group, portando in dote approfondite competenze in ambito networking, data security e collaboration. Si completa così un'offerta votata a rendere la trasformazione digitale efficace, innovativa e sostenibile

Easynet Group e C.I.E. Telematica hanno unito le loro forze per rendere la trasformazione digitale ancor più semplice, efficace, innovativa e sostenibile. C.I.E. Telematica è così diventata una business unit di Easynet Group, che può perciò ora proporre soluzioni per il networking, la collaboration e la sicurezza, che si combinano perfettamente e definiscono il lavoro ibrido come una realtà, dando vita a esperienze inclusive e performanti per tutti i lavoratori, ovunque si trovino.
Parte di una strategia di espansione che ha sempre puntato a rafforzare la

Nella foto da sinistra:
Fabio Meregalli (socio C.I.E. Telematica e Business unit manager), **Alberto Vassena** (Ceo Easynet Group), **Stefania Meregalli** (socia C.I.E. Telematica e marketing manager Easynet Group), **Francesco Missaglia** (Coo Easynet Group) e **Luigi Meregalli** (fondatore di C.I.E. Telematica).

presenza di Easynet nei mercati chiave, l'integrazione di C.I.E. Telematica mira a creare un gruppo ancor più forte, capace di offrire soluzioni integrate e innovative alle aziende, pubbliche e private, ampliando il focus su networking, servizi cloud, data security, collaboration e Internet of Things (IoT), soprattutto in ambito smart city.

Realtà complementari

Easynet Group si è sempre distinta per i suoi servizi gestiti in ambito connettività, cloud e sicurezza informatica. Negli anni ha costruito una solida reputazione come managed service provider in ambito networking e cloud non solo in Italia, ma anche oltre i confini nazionali. Con più di 25 milioni di euro di fatturato nel 2023 (e oltre 30 milioni di euro previsti per l'esercizio 2024), oltre 100 collaboratori e 3 sedi operative (l'headquarter è a Lecco), Easynet Group propone una gamma di servizi e prodotti che abbracciano l'intero panorama IT, dall'intelligenza artificiale all'e-commerce, dalla cybersecurity al cloud computing, includendo anche data center proprietari, il networking e la data analytics.
In oltre 30 di attività, C.I.E. Telematica si è affermata, invece, come punto di riferimento nel panorama italiano delle telecomunicazioni e dei servizi IT. L'azienda ha sviluppato una profonda comprensione del mercato nazionale e ha costruito un portafoglio di servizi su misura per le esigenze specifiche delle aziende italiane e anche della Pubblica amministrazione. Il suo approccio consulenziale genera vere e proprie esperienze di networking e IT per il cliente, che si sviluppano e concretizzano con la selezione tecnologica, la progettazione, l'integrazione di servizi e soluzioni fino alla fornitura.

Poter soddisfare tutte le esigenze

L'ingresso di C.I.E. Telematica in Easynet Group completa la proposta del system integrator lecchese, affiancandosi alle sei business unit già parte del gruppo: **Enforcer** (si occupa di consulenza vendor independent specializzata nelle problematiche di cyber security offensive), **Rgl** (consulenza, assistenza e supporto al management nella strategia di process automation, con un particolare focus in ambito SAP e Salesforce), **Appdigitali** (realizzazione di e-commerce B2B e B2C, siti internet, app, grafica e comunicazione), **E-cloud** (servizi gestiti di cloud computing in logica hybrid cloud), **E-Conn** (servizi gestiti di connettività, networking e VoIP) e **SETA** (formazione in ambito di sicurezza informatica).

Integrazione all'insegna dell'autonomia

L'unione tra Easynet e C.I.E. Telematica consente al gruppo un accesso più ampio al mercato, combinando la presenza internazionale di Easynet Group con la solida base di clienti di C.I.E. Telematica. Infatti, mantenendo l'azienda come business unit se-

parata, Easynet può capitalizzare sulla sua reputazione a vantaggio del brand. Dal canto suo, C.I.E. Telematica mantiene un grado di autonomia operativa, cruciale per rispondere rapidamente alle esigenze specifiche dei clienti.
Questa struttura permette a Easynet Group di stabilire rapidamente una forte presenza nel mercato italiano, accelerando le sfide tipiche dell'espansione organica in un nuovo mercato.

Nuove soluzioni innovative

Easynet Group potenzia così la capacità di ricerca e sviluppo, favorendo l'innovazione in settori come l'IoT, l'intelligenza artificiale e la cybersecurity. Le competenze combinate delle due aziende potranno dare vita a soluzioni innovative che rispondono meglio alle necessità dei clienti.
Easynet Group ha così la possibilità di operare in modo più efficace in un settore sempre più competitivo, offrendo una gamma di servizi più completa e integrata che risponde alle esigenze complesse e articolate delle imprese moderne, dove a fare la differenza sono le proposte di valore e la gestione del servizio.

Un fattore strategico, l'attenzione all'ambiente

Un aspetto che accomuna Easynet e C.I.E. Telematica, e che ha giocato un ruolo chiave nella fusione, è l'attenzione alla sostenibilità: per entrambe è una vera e propria missione. Lo dimostrano le numerose certificazioni ottenute e la qualità dei prodotti e dei servizi. L'attenzione all'ambiente è parte integrante dell'offerta di Easynet Group.
L'operazione Easynet Group con C.I.E. Telematica segna l'inizio di una nuova era per entrambe le aziende. La visione condivisa orientata all'innovazione, all'efficienza operativa, all'espansione del mercato e all'attenzione all'ambiente permette a Easynet Group di ben posizionarsi per affrontare le sfide del futuro e offrire un valore aggiunto ai propri clienti. Easynet Group ha l'obiettivo di trasformare significativamente il panorama tecnologico, creando nuove opportunità e soluzioni per un mondo sempre più connesso e digitale.

Easynet Group investe sul territorio con Quadreria - Digital Academy

La crescente esigenza di figure professionali con competenze specifiche in ambito digitale e tecnologico, in particolare nel campo della cybersecurity e dell'Industria 4.0, ha portato Easynet Group a creare l'innovativo spazio formativo **Quadreria – Digital Academy.**

Ubicata nel territorio lecchese nella storica ex filanda Bovara-Reina di Malgrate, la nuova Academy è dedicata allo sviluppo di competenze digitali e tecnologiche, con un focus sulla cybersecurity, coinvolgendo giovani, professionisti e aziende locali.

Il progetto mira a colmare la carenza di professionalità nel settore IT, creando opportunità formative innovative e immersive per la comunità.

PER SAPERNE DI PIÙ CLICCA QUI

Arrow University 2024: l'evento #EmbraceConnection

Torna il 15 ottobre a Verona la giornata Arrow dedicata a formazione, networking e innovazione per il canale IT

a cura della **Redazione**

Anche quest'anno, la divisione di Arrow Electronics dedicata alle soluzioni Enterprise Computing, organizza in Italia **Arrow University**, l'appuntamento annuale che è dedicato a reseller e system integrator, per favorire l'incontro tra i migliori player del settore IT e offrire loro un'occasione di approfondimento, confronto e networking, oltre a sessioni di formazione.

Il prossimo **15 ottobre, la location di Villa Quaranta, a Ospedaletto di Pescantina (VR)**, aprirà nuovamente le porte alla nuova edizione della Arrow University, un evento che riunirà la maggior parte dei brand a portfolio e molti dei partner di canale di Arrow.

Sarà allestita un'ampia area espositiva dove incontrare i top player del mercato IT e conoscere le soluzioni più innovative del settore. Considerando i messaggi che verranno veicolati durante la University e i forti cambiamenti in atto nel ruolo del canale a valore, Arrow supporterà i partner per aiutarli a trovare le giuste sinergie per la crescita del business. Il tema dell'edizione 2024 sarà **#EmbraceConnection**, **che invita ad abbracciare nuove connessioni, non solo in termini tecnologici, ma soprattutto dal punto di vista umano, in quanto le relazioni e l'espansione del network rappresentano da sempre il vero motore del settore.**

"Ancora una volta siamo entusiasti di risorse ed energie che riusciremo a mettere in campo per la nuova edizione della nostra Arrow University – ha commentato **Michele Puccio, country manager di Arrow Enterprise Computing Solutions in Italia** – *il leitmotiv #EmbraceConnection evidenzia le innumerevoli opportunità che vogliamo offrire ai partner. Nel corso della giornata i reseller potranno sviluppare nuove connessioni con i vari interlocutori del mondo CyberSecurity, Cloud e Next Gen Data Centre, sfruttando tutte le opportunità offerte da Arrow University. Ogni partner potrà partecipare a una molteplicità di speech dei vendor e fare incontri one-to-one ai desk. Non mancheranno momenti di intrattenimento e networking."*

REGISTRATI GRATUITAMENTE QUI

Quantum computing: presente e futuro

Basato sui principi della meccanica quantistica, il calcolo quantistico ha la capacità di risolvere problemi complessi che i computer classici non possono affrontare. Scopriamone lo stato attuale, i principi fondamentali e le applicazioni future

di **Riccardo Florio**

Quando i ricercatori si trovano ad affrontare sfide di grande complessità, spesso si affidano ai supercomputer. Tuttavia, questi strumenti, per quanto avanzati, non sempre riescono a risolvere problemi di portata eccessiva. In questo contesto, i computer quantistici rappresentano un'alternativa rivoluzionaria, sfruttando i principi della fisica quantistica per affrontare questioni che i metodi di calcolo convenzionali non riescono a gestire.

I computer quantistici si basano su tre concetti fondamentali della meccanica quantistica: sovrapposizione, entanglement e interferenza. Questi principi conferiscono ai computer quantistici una capacità di elaborazione che supera di gran lunga quella dei computer classici, i quali operano in modo diverso, utilizzando bit binari per trasmettere informazioni.

I computer quantistici, invece, utilizzano i **qubit, particelle subatomiche come elettroni o fotoni che possono esistere in stati di sovrapposizione**, conferendo ai computer quantistici un potenziale analitico straordinario.

Un funzionamento basato sui qbit

Un qubit, abbreviazione di “quantum bit”, è l’unità fondamentale di informazione nel calcolo quantistico, analogamente a come il bit è l’unità di informazione nei computer classici.

In un sistema classico, un bit può avere solo due stati e può essere rappresentato come un interruttore che è acceso (1) o spento (0). Un qubit, invece, esistere simultaneamente in una combinazione di entrambi gli stati, grazie alle proprietà della meccanica quantistica, in particolare il **principio di sovrapposizione** quantistica. Questo significa che, fino a quando non viene misurato, un qubit non è né 0 né 1, ma può essere considerato come se fosse entrambi gli stati contemporaneamente.

Quando un qubit viene misurato lo stato di sovrapposizione viene distrutto e il qubit collassa, assumendo uno stato ben definito, 0 oppure 1, e perdendo la sua natura quantistica.

Un’altra proprietà fondamentale di un qubit è l’**entanglement**, che si verifica quando due o più qubit diventano correlati in modo tale che lo stato di uno dipende istantaneamente dallo stato dell’altro, indipendentemente dalla distanza che li separa. Questo fenomeno, che Einstein definì come “azione spettrale a distanza”, permette di creare correlazioni tra qubit che non hanno equivalente nei sistemi classici e che sono fondamentali per molti algoritmi quantistici.

GLI APPROFONDIMENTI DI BIZZIT

Il Quantum Computing italiano è una questione di fisico

L’Italia dei quanti ha le idee chiare ed è pronta alla crescita. Che dipenderà molto dall’intelligenza delle aziende

continua a leggere

L’interferenza quantistica è un altro fenomeno che gioca un ruolo cruciale nel comportamento dei qubit. Quando i qubit esistono in uno stato di sovrapposizione, le probabilità di vari risultati possono interferire tra loro, rafforzandosi o annullandosi. Questo principio può essere sfruttato per progettare algoritmi quantistici in modo che gli stati “corretti” siano amplificati, mentre quelli “errati” siano cancellati, portando a una soluzione più efficiente rispetto al calcolo classico. **I qubit possono essere realizzati utilizzando diverse tecnologie fisiche**: tramite circuiti superconduttori che esibiscono proprietà quantistiche a basse temperature, intrappolando e manipolando atomi ionizzati utilizzando campi elettromagnetici, utilizzando la polarizzazione dei fotoni

per rappresentare lo stato quantico e sfruttando lo spin degli elettroni in materiali semiconduttori. Ogni tecnologia ha i suoi vantaggi e svantaggi, e la ricerca continua a esplorare quale sarà la più efficace per lo sviluppo di computer quantistici su larga scala.

COS'È UN QUBIT ?

I computer quantistici

I computer quantistici elaborano le informazioni in modo fondamentalmente diverso rispetto ai computer classici. Utilizzano una serie di algoritmi per eseguire osservazioni e misurazioni, creando uno spazio multidimensionale che contiene dati e schemi complessi.
Un computer quantistico reale è fisicamente composto da tre componenti principali.
Un **computer convenzionale** e il suo hardware di supporto che si occupano della programmazione e della comunicazione dei comandi ai qubit.
Una **sistema per trasmettere segnali** dal computer ai qubit.
Un'**unità di archiviazione dei qubit** che deve essere in grado di stabilizzare i qubit e deve soddisfare una serie di requisiti o condizioni che possono prevedere l'alloggiamento della camera a vuoto o richiedere temperature prossime allo zero.
Tuttavia, uno dei problemi principali è che le proprietà quantistiche dei qubit si deteriorano dopo un certo numero di operazioni e la maggior parte delle applicazioni di calcolo quantistico richiede che migliaia o milioni di qubit lavorino insieme senza perdere il loro comportamento quantistico.

Il processore quantistico

Il cuore di un computer quantistico è il **processore quantistico**, che può assumere diverse forme, come i processori fotonici, spintronici o a trappola ionica. Recentemente, i processori a trappola ionica hanno dimostrato di offrire un migliore isolamento dei qubit e una maggiore potenza di elaborazione con un numero inferiore di qubit rispetto ad altri tipi di processori. Questi processori sono costituiti da un chip fisico, chiamato unità di elaborazione quantistica (QPU), che contiene una serie di qubit interconnessi. I **circuiti quantistici**, che costituiscono la base del calcolo quantistico, sono composti da un registro a n-qubit e una serie di porte quantistiche collegate da "fili". La "larghezza" fissa del circuito è determinata dalla quantità di qubit da elaborare. I circuiti superconduttori sono utilizzati per trasferire i dati in ingresso e in uscita da un processore quantistico a un dispositivo di lettura e, per funzionare correttamente, devono essere raffreddati a temperature estremamente basse (circa 10 mK).
Un **processore quantistico** è un dispositivo complesso che sfrutta le proprietà della meccanica quantistica. A differenza dei processori classici, che utilizzano transistor per

manipolare bit in stati di 0 o 1, i processori quantistici manipolano qubit, in grado di rappresentare simultaneamente sia 0 che 1 grazie alla sovrapposizione quantistica.
Per manipolare i qubit, il processore è dotato di **unità di controllo e manipolazione**. Queste unità includono circuiti e hardware specializzati che generano impulsi di microonde, campi magnetici o laser, utilizzati per controllare lo stato dei qubit. Attraverso questi impulsi, il processore esegue operazioni specifiche, note come porte quantistiche, che svolgono un ruolo simile alle porte logiche nei processori classici.
Dopo che un calcolo quantistico è stato completato, il processore deve misurare lo stato dei qubit per ottenere un risultato leggibile. I circuiti di lettura svolgono questa funzione, convertendo lo stato quantico dei qubit in un output classico, tipicamente 0 o 1. Questo processo di misurazione, però, distrugge la sovrapposizione, facendo collassare il qubit in uno dei due stati classici. Poiché i processori quantistici richiedono condizioni estremamente precise per funzionare correttamente, è necessario mantenere temperature estremamente basse, spesso vicine allo zero assoluto (-273°C).
Per raggiungere queste condizioni, il processore è dotato di un sistema di raffreddamento avanzato che è essenziale per preservare le delicate proprietà quantistiche che permettono al processore di eseguire calcoli che sarebbero impossibili per i computer.

Sfide e prospettive future

Sebbene il quantum computing abbia un grande potenziale, ci sono alcuni ostacoli che devono essere superati e su cui accademici e sviluppatori stanno lavorando. Uno dei problemi principali è che i qubit sono altamente sensibili alle influenze esterne, che portano alla **de-coerenza, in cui i qubit perdono il loro stato quantico e diventano bit classici.** Per un'elaborazione quantistica accurata, è essenziale mantenere la stabilità dei qubit e ridurre al minimo la de-coerenza.
Inoltre, i computer quantistici sono soggetti a errori a causa della fragilità intrinseca dei qubit. Una computazione quantistica affidabile richiede l'uso di circuiti

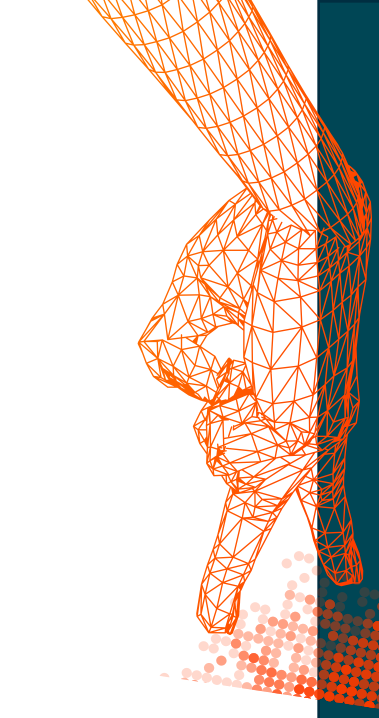
GLI APPROFONDIMENTI DI BIZZIT

Rendere possibile l'impossibile

L'evoluzione della capacità di calcolo porterà a risolvere problemi che oggi non si può nemmeno pensare di affrontare.

continua a leggere

quantistici tolleranti agli errori e la correzione degli errori.
Va poi ricordato che la costruzione di computer quantistici pratici e su larga scala è ancora una sfida significativa. Le attuali implementazioni hardware incontrano limitazioni nel numero di qubit, nella connettività e nei tassi di errore. Sono necessari sviluppi nell'hardware quantistico per creare sistemi quantistici scalabili e potenti. È impegnativo progettare e programmare i computer quantistici.
In più **i costi associati sono molto elevati:** l'hardware quantistico è costoso, la supply chain complesse, vulnerabili e costose da creare e mantenere. Affrontare queste spese e trovare investimenti per compensarle sarà probabilmente un compito standard degli scienziati istituzionali e degli imprenditori commerciali per il prossimo futuro.
Altri aspetti riguardano **lo sviluppo del software** poiché gli algoritmi quantistici e gli strumenti di sviluppo del software sono ancora agli albori e c'è bisogno di nuovi linguaggi di programmazione, compilatori e strumenti di ottimizzazione in grado di utilizzare efficacemente la potenza dei computer quantistici.
I computer quantistici **non sostituiranno i computer classici, ma saranno una tecnologia complementare.** Lo sviluppo di metodi efficienti e affidabili per il trasferimento di dati tra computer classici e quantistici è essenziale per le applicazioni pratiche. La maturazione del campo dell'informatica quantistica richiederà anche la definizione di nuovi standard e protocolli per l'hardware, il software e le interfacce di comunicazione.
Infine non ci sono molte persone nel mondo che hanno ricevuto l'**istruzione e la formazione necessarie per entrare nella forza lavoro quantistica.** Un maggior numero di persone sarà spinto a entrare nella forza lavoro quantistica prima che ci siano più computer quantistici pratici, e non ci saranno più computer quantistici pratici finché non ci saranno più persone motivate a entrare nella forza lavoro quantistica.
Il futuro dell'informatica quantistica è allo stesso tempo entusiasmante e incerto. Realizzare computer quantistici pratici che superino i computer classici per una serie di applicazioni è ancora una sfida, nonostante il fatto che l'informatica quantistica abbia già raggiunto risultati rivoluzionari. Tuttavia, l'aumento dei finanziamenti e le continue attività di ricerca e sviluppo stanno facendo progredire le capacità delle tecnologie quantistiche.
Nei prossimi cinque-dieci anni potremmo assistere a importanti progressi nell'hardware quantistico, nei metodi di correzione degli errori e nei nuovi algoritmi quantistici. Con questi sviluppi, i ricercatori, le imprese e, in ultima analisi, la società in generale potrebbero trovare l'informatica quantistica più accessibile.



LE APPLICAZIONI DEL CALCOLO QUANTISTICO

Il calcolo quantistico ha il potenziale per trasformare molti settori.

SERVIZI FINANZIARI
Nei servizi finanziari, potrebbe permettere la creazione di portafogli di investimento più efficienti e redditizi, migliorando la rilevazione delle frodi e ottimizzando i simulatori di trading.

CRITTOGRAFIA
Nel campo della crittografia, i computer quantistici sono in grado di decrittare dati cifrati con tecniche utilizzate dai computer tradizionali, rendendo necessaria una nuova generazione di tecniche crittografiche. Inoltre, il calcolo quantistico potrebbe rivoluzionare la scoperta di farmaci, permettendo di confrontare molecole complesse e riducendo significativamente il tempo e i costi associati allo sviluppo di nuovi trattamenti.

INTELLIGENZA ARTIFICIALE
Nell'intelligenza artificiale e nel machine learning, il calcolo quantistico potrebbe accelerare l'ottimizzazione, la classificazione dei dati e l'addestramento dei modelli, riducendo i tempi di sviluppo delle applicazioni.

SUPPLY CHAIN E NELLA LOGISTICA
Nel settore della supply chain e della logistica, i computer quantistici potrebbero migliorare l'efficienza delle rotte di trasporto, ridurre i tempi di viaggio e migliorare la gestione dell'inventario.

MODELLIZZAZIONE CLIMATICA
Nella modellizzazione climatica, i computer quantistici potrebbero migliorare la velocità e la precisione delle previsioni meteorologiche, cruciali per comprendere i cambiamenti climatici e sviluppare strategie di mitigazione. Le comunicazioni quantistiche e il settore aerospaziale potrebbero beneficiare della potenza di calcolo quantistica per migliorare i sistemi di controllo del traffico aereo e le operazioni militari.

CONTROLO DEL TRAFFICO
Anche il controllo del traffico nelle città potrebbe trarre vantaggio dai computer quantistici, riducendo i tempi di attesa e mitigando gli ingorghi. In ambito pubblicitario e di marketing, gli algoritmi quantistici potrebbero migliorare l'efficacia delle campagne pubblicitarie, basandosi su fattori come le risposte emotive degli utenti e la creazione di relazioni a lungo termine con i clienti.

MANIFATTURIERO
Nel settore manifatturiero, i computer quantistici potrebbero migliorare la prototipazione e i test, riducendo i costi e ottenendo design più efficienti, mentre nel campo delle batterie, il calcolo quantistico potrebbe fornire una maggiore comprensione della chimica delle batterie e dei composti di litio, portando a miglioramenti nelle batterie per veicoli elettrici.

Il mondo cambia, il cyber cambia

di **Maurizio Ferrari**

Gli attuali conflitti stanno ridisegnando gli equilibri geopolitici mondiali e queste guerre si stanno combattendo anche nel cyberspazio. Ne parlano Lucio Caracciolo, direttore di Limes, e Pierguido Iezzi di Tinexta Cyber

Stiamo vivendo in un'epoca di grandi cambiamenti, il sistema geopolitico ed economico che dal dopoguerra ha "dominato" il mondo, capeggiato dagli Stati Uniti, è in forte crisi. È uno scenario particolare che apre le porte a nuove sfide. **Tinexta Cyber**, importante realtà italiana attiva nella cybersicurezza, ha chiesto a **Lucio Caracciolo, fondatore e direttore della rivista Limes**, di fare una foto-

Lucio Caracciolo,
fondatore e direttore
della rivista Limes

grafia di quello che sta succedendo e come l'Italia ne è coinvolta. Secondo Caracciolo il mondo come lo abbiamo conosciuto sta cambiando in modo radicale e si stanno ridisegnando gli equilibri geopolitici a livello globale e locale. Con locale si intende Europa e Italia. Il direttore di Limes ha evidenziato nella crisi della Lehman Brothers nel 2008 il punto d'innesco della deflagrazione della fine del mondo sotto il controllo degli Usa. Il gigante ha mostrato di essere debole e questo ha fatto alzare la testa alla Russia e alla Cina, in primis, e poi ad altri Paesi come India e quelli Medio Orientali. Il mondo delle regole, di cui gli Stati Uniti erano i guardiani, è pian piano crollato, lasciando spazio a un mondo dove il più forte impone le proprie ragioni.

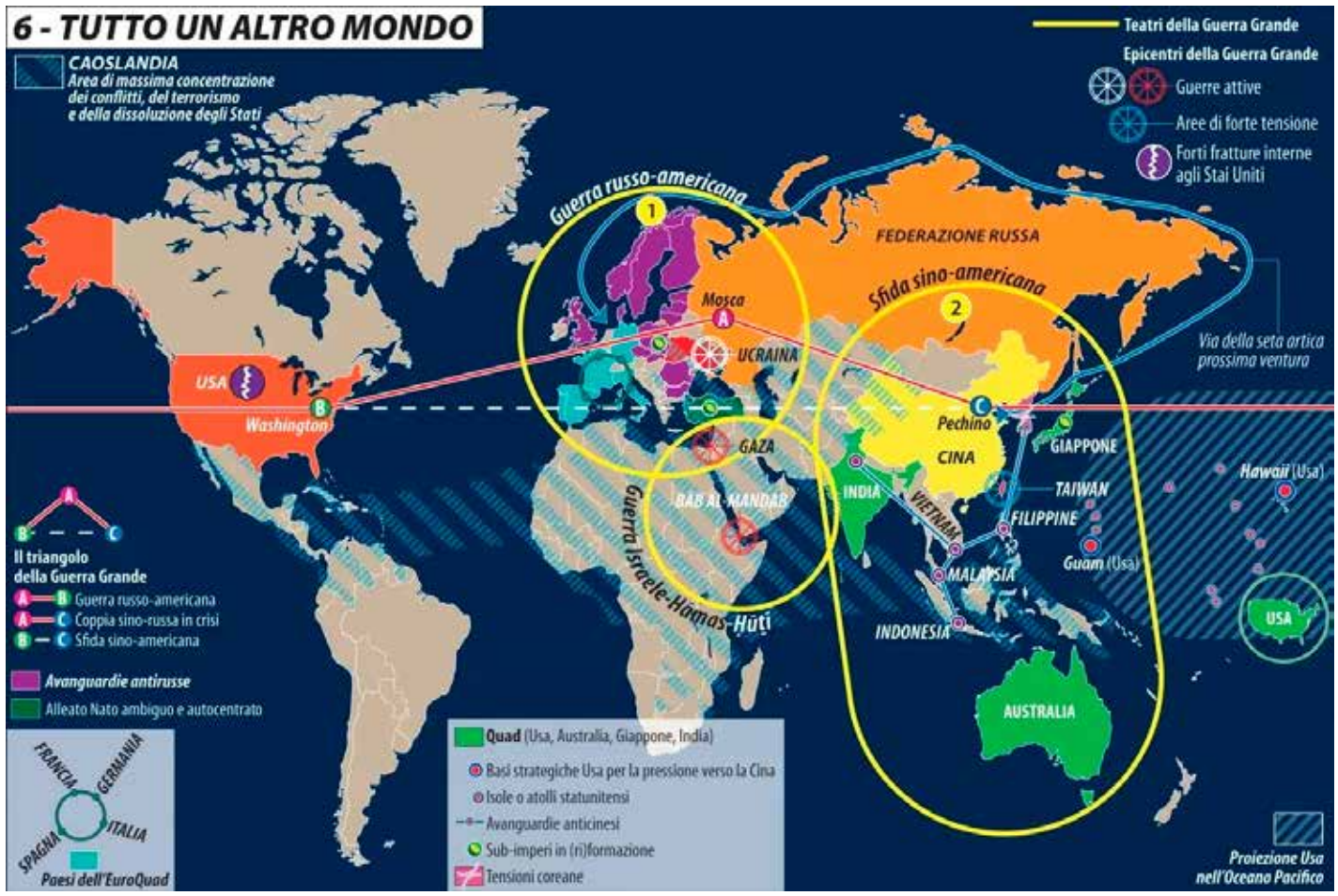
Lo spettro della guerra in Europa

L'attacco della Russia all'Ucraina è il culmine di questo processo, dove la diplomazia e la politica sono state sostituite dalle armi. Attacco che ha riportato sull'Europa lo spettro della guerra: si combatte a meno di 2000 chilometri dall'Italia. Questa non è la sola guerra in corso e nemmeno l'unico punto di crisi, in questo momento si combatte in Medio Oriente, con Israele impegnato in una guerra a Hamas, o meglio all'Iran, la nazione che sta sponsorizzando questo conflitto. C'è anche la questione Cina - Taiwan, che apre il fronte del controllo delle rotte commerciali nell'Oceano Pacifico. Perché se la Russia sta mettendo pressione sull'Europa, la Cina sta lavorando per diventare la potenza che controllerà le rotte commerciali negli Oceani Indiano e Pacifico, e per farlo vuole scalzare gli Usa e i suoi alleati, Australia, Nuova Zelanda, Giappone e, in questo ambito, India. Quest'ultima e la Cina cercano di giocare su più tavoli per trarre il massimo profitto dalla situazione di tensione che si è creata con l'azione Russa in Ucraina. Questa non è altro che la superficie dell'iceberg; oggi, secondo Caracciolo, le superpotenze mondiali si stanno sfidando in diversi ambiti: Terra,

Pierguido Iezzi,
strategic business
development Tinexta Cyber

Cyberspazio il futuro fronte

Il cyber è il "nuovo" territorio dove si sta combattendo. **Pierguido Iezzi, strategic business development Tinexta Cyber**, è intervenuto spiegando come una nazione, in questo ambito, deve mettere in campo le risorse per avere una capacita offensiva, difensiva e un forte intelligence. I conflitti tra Russia e Ucraina, e Israele ed Hamas hanno messo in luce come questi conflitti oggi siano combattuti su diversi fronti: una guerra multidominio dove il cyber è protagonista. Ai gruppi di hacker che adottano ransomware per bloccare e ricattare le strutture occidentali (una curiosità: se nel sistema da infettare c'è una tastiera in cirillico dei ransomware non si attivano), si stanno aggiungendo gruppi che utilizzano wiper, che cancellano i dati senza chiedere soldi, per causare più danni possibile. Diventa difficile stabilire se dietro questi gruppi c'è o non c'è uno stato sponsor, ma sicuramente molti hanno accesso a risorse non indifferenti. Il panorama, secondo Iezzi, sì è ulteriormente allargato e non si può più parlare solo di sicurezza informatica. Attraverso dei gruppi di attivisti gli attori in gioco, sfruttando al meglio i social e i canali di comunicazione del web, veicolano e diffondono notizie per creare movimenti d'opinione, a volte mirati a destabilizzare la società dal suo interno. Oggi basta una computer, una connessione e un po' di competenza per fare dei danni. Sul campo di gioco si possono trovare dei mercenari che si offrono al miglior offerente, come dei cani sciolti che estremizzati operano in modo indipendente per colpire chi ritengono il nemico. Il controllo delle informazioni è diventato dunque fondamentale e, spiega Iezzi, per non rischiare di farsi trovare impreparata all'evoluzione cyber della guerra l'Europa si sta dotando di norme e regolamenti, come la NIS2, per alzare il livello di sicurezza in tutti i Paesi dell'Unione, coinvolgendo non solo le realtà apicali, ma tutta la filiera così da non lasciare spazi facilmente attaccabili e tutelare l'Identità Europea e lo spazio cyber dell'Europa.
Da questo caos nascerà un nuovo sistema mondiale dove l'Europa, e l'Italia in particolare, che in questo momento è in una situazione geopolitica molto difficile, dovranno trovare il loro ruolo. Caracciolo ha sottolineato come il Mediterraneo sia al centro di forti tensioni. Diversi Paesi che si affacciano su questo Mare vogliono estendere unilateralmente la Zona economica



esclusiva, senza dimenticare come l'area del Mar Rosso, con il canale di Suez in difficoltà per le azioni di pirati e di gruppi terroristici sponsorizzati dall'Iran che attaccano le navi in transito. Questa situazione può portare a un rallentamento dei traffici marittimi verso l'Europa, e soprattutto verso l'Italia, dirottandoli verso aree più sicure (come i porti che danno sull'Oceano Atlantico e Amburgo). Un altro problema è il calo demografico a cui sta andando incontro il mondo occidentale e l'Italia in particolare; calo demografico che sta aprendo le porte all'immigrazione per riuscire a mantenere la produzione. L'alternativa è la sostituzione della forza lavoro con robot e intelligenza artificiale. Quest'ultima è una prospettiva difficilmente realizzabile, anche se l'automazione sarà sempre più presente nelle realtà colpite da questo fenomeno. Caracciolo ha sottolineato, inoltre, come l'Africa sia diventata terra di conquista per Russia e Cina, che stanno usando questo continente per i loro scopi sia politici sia economici. Siamo dunque in prima fila nell'assistere al cambiamento di questa società che alla fine dovrà ritrovare il proprio equilibrio.

L'APPROFONDIMENTO

Piattaforme di sicurezza dei dati: presente e futuro

In uno scenario in cui le minacce sono sempre più efficaci, i trend di mercato indirizzano verso l'adozione di modelli di sicurezza basati su piattaforme capaci di mettere a fattor comune non solo differenti tecnologie ma anche soluzioni di terze parti.

continua a leggere

L’IT Asset Management è automatico con Know & Decide

di **Leo Sorge**

Licenze ed acquisti, green IT o Nis2 richiedono di semplificare il controllo, aumentare la sicurezza e ottimizzare l’inventario. Queste operazioni possono essere svolte in modo automatico non solo da software dell’IT interna, ma anche tramite piattaforme SaaS già pronte all’uso

L’assessment delle proprietà ICT è da sempre la più trascurata delle fasi. Hardware, software e servizi si affastellano gli uni sugli altri, spesso affidando la realizzazione a un partner che ha una visione completa del parco complessivo. L’esatta conoscenza del parco permette di ottimizzare i costi in maniera decisa, migliorando la sicurezza ed evitando tutta una serie di inefficienze oggi non correttamente considerate (si pensi all’assegnazione di una nuova postazione di lavoro).

Finora questa fase è rimasta una foto sbiadita dal tempo. Andando verso driver di mercato come Nis2 o obiettivi Esg, l’approccio verso soluzioni di asset management in tempo reale sta rapidamente cambiando in tutti i mercati: si richiede un elenco preciso e in tempo reale o quasi. **GlobalView è una soluzione di IT Asset Management (Itam) completamente automatizzata** per controllare, proteggere e ottimizzare il patrimonio

informatico, aiutando a prendere decisioni IT migliori. Visibilità e controllo portano a risparmi consistenti ma soprattutto a un funzionamento ottimale dell'intero inventory hardware e software, compresi aspetti di sicurezza. L'idea è nata nel 2015, durante la consulenza a un cliente con esigenze di backup. *"Quando gli ho chiesto quante postazioni di lavoro erano interessate e quale capacità fosse prevista, il cliente non seppe darmi una risposta precisa"*, racconta **Emmanuel Moreau, Ceo & co-founder di Know & Decide**. Diventò chiara l'importanza di una soluzione automatizzata, sulla quale il Ceo iniziò subito a lavorare insieme a Nicolas Trotot. Il software di K&D offre una visione unificata di tutti i CI (Configuration Item), inclusi hardware, software, elementi virtuali, documentazione e personale. Il software automatizza la discovery e l'identificazione di tutti i CI, compresi quelli dimenticati o trascurati. *"Una volta abbiamo scovato una Playstation attaccata alla rete aziendale"*, ha detto Moreau. Certo ci sarebbe Active Directory, ma la qualità dei dati è piuttosto variabile e l'elenco non è completo. GlobalView, invece, permette di ridurre i costi IT fino al 30% il primo anno e di almeno il 5% ogni anno successivo, ottimizzando le licenze software, identificando i CI obsoleti e automatizzando i processi IT. *"I grandi editori di software non sono molto interessati a questa nicchia, per cui non competono con noi* - spiega il Ceo dell'azienda lussemburghese *-; i nostri competitor sono i reparti ICT di ciascuna azienda, che in genere, per molti motivi, sviluppano internamente questo tipo di software"*.

Emmanuel Moreau
Ceo & co-founder
di Know & Decide

Questa suite, integrabile con eventuali strumenti già all'opera, permette di trasformare il reparto IT da un centro di costo a un centro di servizi. L'azienda si trova un portale web decisionale che permette di indirizzare le scelte, dalla protezione di un server o di una postazione di lavoro correttamente in elenco alla gestione del ciclo di vita a partire dalla data di acquisto.

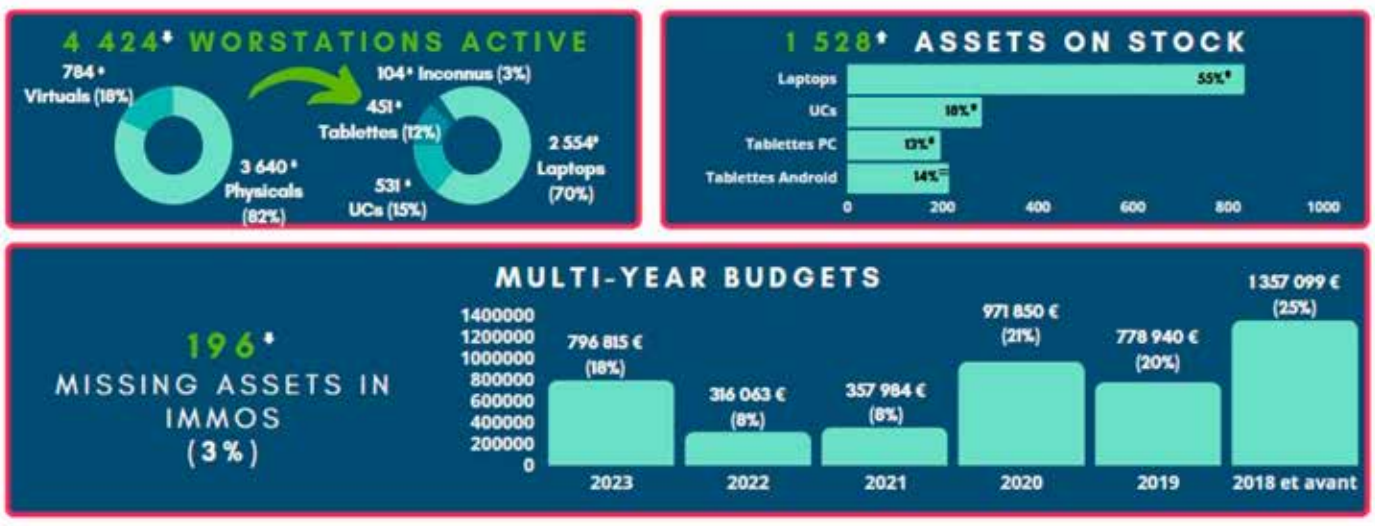
Una possibilità per il canale

L'azienda è alla ricerca di partner: *"Abbiamo effettuato le prime vendite dirette a importanti clienti in Belgio, Lussemburgo e Francia* - ha spiegato Moreau *-; il nostro profilo di partner abbraccia mercati verticali come la gestione patrimoniale, l'ITSM (IT service management) e la Green IT"*.
Nell'ambito della campagna di reclutamento del canale, l'azienda è alla ricerca di Var, Oem, integratori di sistema e distributori. Il prodotto viene venduto con un abbonamento triennale e si basa sul numero di CI controllati dal sistema Itam.

Il costo annuale per CI varia a seconda del numero di CI presenti nella gamma da 1 a 10 euro.
La soluzione è composta dai tre moduli di data discover, data management e data report. Il modulo di scoperta è un'applicazione basata sul Web per automatizzare la raccolta dei dati grazie a più di 80 connettori tramite Api; comprende anche una funzionalità di importazione di file per tutti i documenti offline relativi a risorse IT come file finanziari o contrattuali. Il modulo si collega anche agli ERP e ad altri cataloghi di riferimento simili che vanno ad alimentare il database di configurazione, CMDB (configuration manager database).
La gestione è realizzata con un motore di regole del linguaggio naturale per configurare regole e controlli, mentre i rapporti sono ottenuti da un portale web che crea dashboard in pochi clic. Tra i casi d'uso più frequenti troviamo la visione globale di tutte le risorse IT, la qualità del CMDB, il piano di produzione, il piano di sicurezza e il modello di costo. Certamente altre specifiche necessità possono essere risolte con un sistema di questo tipo.

Audit hardware e software in ore

Dal punto di vista operativo, tutti i dati vengono consolidati, raggruppando tutti gli attributi tecnici, funzionali e finanziari dei CI in un unico repository centralizzato, ideale per consultazione e analisi. La completa gestione del ciclo di vita dei CI dalla scoperta alla dismissione offre tre vantaggi fondamentali su licenze, obsolescenza e automazione. Ottimizzare l'uso delle licenze permette di non pagare per ciò che non viene effettivamente usato, o di integrare eventuali carenze. Eliminare i CI obsoleti, non più necessari o supportati, libera risorse e riduce i rischi. Automatizzare attività ripetitive come la patch management e la configurazione dei dispositivi permette di risparmiare tempo e migliorare l'efficienza; assicurarsi che tutti i CI siano protetti da antivirus, backup e altri strumenti di sicurezza essenziali garantisce un servizio IT affidabile e performante.
GlobalView è una soluzione SaaS che si integra con i principali strumenti IT, come CMDB, AD e strumenti di sicurezza. Know & Decide offre ai clienti una prova gratuita e piani di abbonamento flessibili.



Un caso di studio sulla gestione del budget

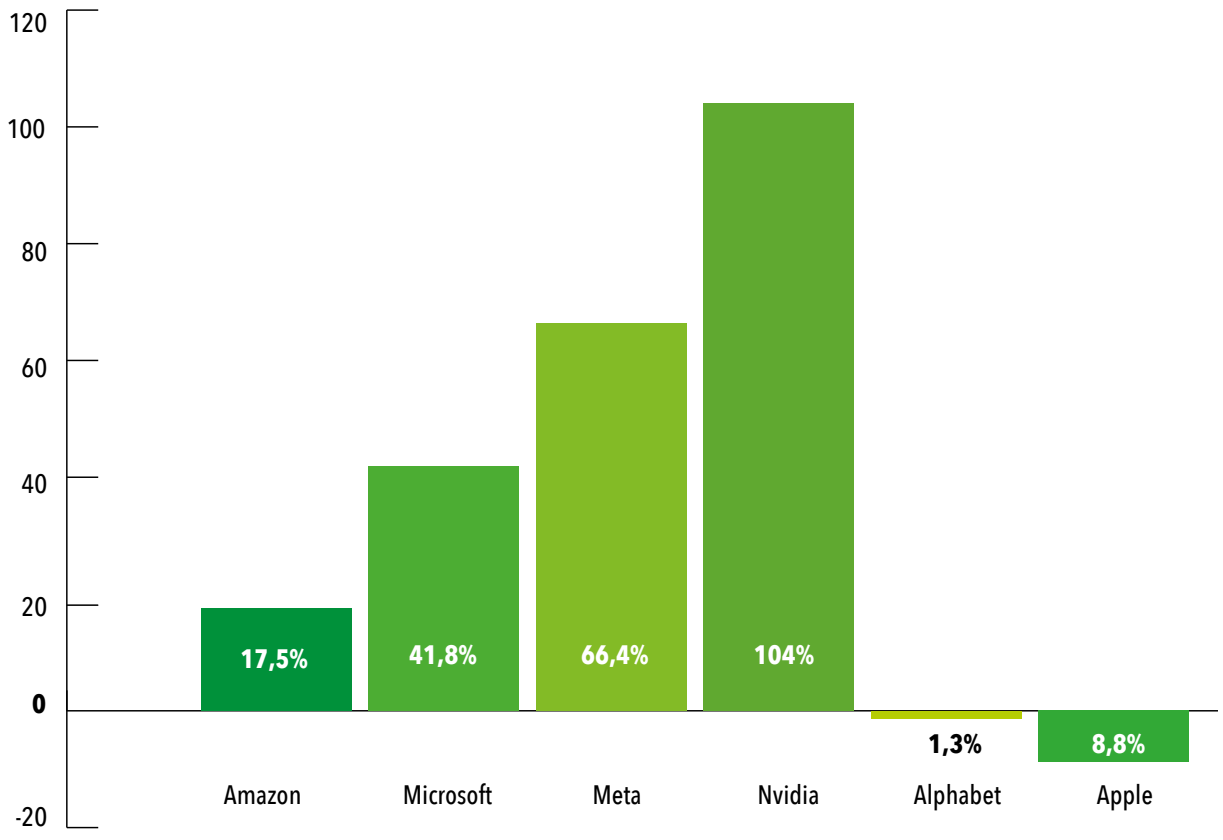
La sostenibilità digitale delle Big tech

di **Maurizio Ferrari**

Il web impatta sul pianeta come se fosse una nazione. La sostenibilità digitale, con l'avvento dell'AI, è un tema da approfondire. Le Big tech consumano più energia elettrica del Belgio e del Cile. Il Report di Karma Metrix

La Giornata Mondiale dell'Ambiente rappresenta un'occasione annuale per riflettere e sensibilizzare sull'impatto che le attività umane, comprese quelle nel mondo digitale, hanno sul nostro pianeta. Per far capire gli effetti del web e del mondo della tecnologia sul pianeta, **Karma Metrix** ha presentato i risultati del 3° Rapporto 2024 dell'**Osservatorio ESG Big Tech** che mostra come le sei più importanti società che operano nel settore del web e della tecnologia – **Amazon, Apple, Meta, Alphabet, Microsoft e Nvidia** – si possano equiparare a una nazione per quanto riguarda i consumi elettrici e la produzione di CO_2 equivalente. Se si considera tutto il mondo del web i numeri sono "impressionanti", come spiega il professor **Roberto Razeto dello Iulm**: *"Se il web fosse una nazione, secondo il Global Carbon Project sarebbe il 3° Paese al mondo per consumo di energia elettrica e il 4° per le*

emissioni di CO_2. Purtroppo molta gente, circa il 60%, ignora completamente che navigare su Internet provochi l'emissione di CO_2 (Fonte - Sharethrough "Consumer Understanding of Internet Carbon Emissions", maggio 2022 - *ndr*)".
Karma Metrix, in collaborazione con il Micri (Master in comunicazione per le relazioni internazionali) dello Iulm, ha analizzato i report sulla sostenibilità delle principali società che operano sul web, con un focus sull'intelligenza artificiale. Quest'ultima è uscita definitivamente dai laboratori di ricerca per entrare nel mercato, tanto che oggi è l'elemento caratterizzante per il marketing delle aziende. Ma, numeri alla mano, **l'intelligenza artificiale consuma molta energia elettrica**, tanto che le società attive in questo settore hanno visto aumentare i loro consumi energetici in modo significativo. L'inserimento in questa ricerca di Nvidia è legato proprio all'utilizzo delle sue GPU nel mondo AI. Queste sei società capitalizzano qualcosa come 13,5 trilioni di dollari: per dare un parametro di confronto l'Italia ha un Pil di 2,08 trilioni di dollari nel 2023. Insieme sono il 50° Paese al mondo per emissioni di CO_2: con 130,1 milioni di tonnellate si piazzano tra il Cile e la Repubblica Ceca, mentre dal punto di vista dei consumi elettrici arrivano a essere il 37° Paese al mondo con 91 milioni di MWh, sopra Finlandia, Belgio, Cile. Se nel mondo il consumo elettrico cresce del 3%, in queste big tech cresce del 18,4%. Scendendo nel dettaglio, come detto prima, **le società più attive nell'AI hanno fatto segnare gli incrementi di consumo elettrico e di emissioni di CO_2 più significativi**; analizzando i dati



disponibili per tutti (2020, 2021, 2022) le emissioni di CO_2 sono così aumentate: Amazon +17,5%, Microsoft +41,8%, Meta +66,4% e Nvidia +104%. Chi ha "rallentato" il lavoro sull'AI ha, invece, diminuito le proprie emissioni: Alphabet -1,3% e Apple -8,8%. Un discorso a parte va dedicato al **consumo di acqua destinato al raffreddamento dei data center**, che è in costante crescita: tra il 2019 e il 2022 **è aumentato del 63%**. Per contenerlo diverse società hanno elaborato specifiche attività per il riciclo e il recupero, così da essere meno impattanti su una risorsa importante come l'acqua. Tutte le Big tech hanno sviluppato programmi per aumentare il ricorso a energie rinnovabili e diminuire di conseguenza la propria impronta di carbonio, anche se su tutte loro rimane l'incognita AI, che è una tecnologia affamata di risorse. Karma Metrix ha sviluppato un servizio, fornito in modalità Saas, che consente di analizzare la sostenibilità digitale di un sito web e di calcolare quanta CO_2 equivalente emette. In questo modo per le società è possibile avere una metrica certa di quanto sia impattante la navigazione sul proprio sito e apportare gli opportuni correttivi, così da ridurre le emissioni di CO_2 e migliorare la propria sostenibilità digitale.

ANALIZZA LA SOSTENIBILITÀ DIGITALE DEL TUO SITO WEB

Ale Agostini
Ceo di Karma Metrix

L'obiettivo per il futuro di Karma Metrix è espandere questo servizio anche ad altri sistemi aziendali, come la posta elettronica. La "nazione" del Web deve, come spiega **Ale Agostini, Ceo di Karma Metrix**, *"risparmiare e limitare le emissioni di CO_2 derivanti dalle tecnologie digitali fino a quando non avremo solo fonti di energia pulite"*.

GLI APPROFONDIMENTI DI BIZZIT

Data center energivori: serve un cambio di passo sostenibile

Le preoccupazioni espresse dalle Nazioni Unite in merito all'impatto ambientale del settore data center sono fondate su dati concreti. Nonostante gli impegni assunti da colossi come Google e Microsoft per raggiungere il "net zero" entro la fine del decennio, si osservano trend preoccupanti.

CONTINUA A LEGGERE

Stampa connessa: elemento chiave nella digital transformation

La stampa connessa rappresenta un'area dinamica dell'IT che offre opportunità per migliorare sicurezza, gestione documentale e sostenibilità, aumentando l'efficienza e riducendo i costi operativi

di **Riccardo Florio**

Il mercato della stampa, tradizionalmente visto come statico e maturo, sta attraversando una fase di trasformazione significativa grazie all'integrazione delle tecnologie digitali. **Secondo gli ultimi dati degli analisti di IDC, il mercato globale della stampa**, che comprende stampanti, multifunzione (MFP) e soluzioni di gestione dei documenti, ha registrato un valore di circa 135 miliardi di dollari nel 2023, con previsioni di crescita moderata nei prossimi anni, raggiungendo i **140 miliardi di dollari entro il 2027**.

Tuttavia, sempre secondo IDC, il segmento della stampa connessa, che include soluzioni basate su cloud e dispositivi IoT, sta mostrando tassi di crescita molto più elevati, con un CAGR (tasso di crescita annuale composto) previsto del **10,2% fino al 2028**.
Questa crescita è trainata da una crescente domanda di soluzioni che integrino la stampa tradizionale con le più recenti innovazioni tecnologiche, offrendo una maggiore efficienza e un controllo più preciso dei processi di stampa e gestione documentale.

GLI APPROFONDIMENTI DI BIZZIT

Stampa 4.0: integrazione e automazione nel cuore del business

La stampa è un processo sempre più integrato nel flusso di lavoro aziendale e, grazie anche all'impiego delle tecnologie più attuali, come l'IoT, il cloud e l'intelligenza artificiale, può rivestire un ruolo strategico per il business.

continua a leggere

Le aziende stanno, infatti, investendo in stampanti intelligenti che si integrano con le infrastrutture IT esistenti, permettendo una gestione centralizzata e l'ottimizzazione delle risorse, rispondendo alle esigenze di un mercato sempre più orientato verso la digitalizzazione.

La stampa connessa

La stampa connessa è un'evoluzione tecnologica del tradizionale processo di stampa, che integra dispositivi di stampa come stampanti e multifunzione (MFP) con le infrastrutture digitali esistenti, come reti aziendali, servizi cloud e tecnologie IoT (Internet of Things). Questa integrazione consente non solo di migliorare l'efficienza operativa, ma anche di offrire nuove funzionalità e servizi che vanno oltre la semplice produzione di documenti cartacei.

In un contesto di stampa connessa, i dispositivi non sono più entità isolate che ricevono comandi da singoli computer; al contrario, fanno parte di un ecosistema digitale più ampio in cui comunicano tra loro e con altri sistemi aziendali. Questa connessione avviene attraverso reti cablate o wireless e permette di gestire centralmente le operazioni di stampa, monitorare in tempo reale lo stato dei dispositivi, raccogliere dati per l'analisi dei flussi di lavoro e ottimizzare l'uso delle risorse.

Innovazione tecnologica e trend emergenti

Il settore della stampa connessa sta beneficiando di diverse innovazioni tecnologiche che stanno ridefinendo l'intero panorama; **l'integrazione con il cloud, l'adozione dell'Internet of Things (IoT) e l'intelligenza artificiale (AI)** permettono lo sviluppo di soluzioni di stampa più intelligenti, capaci di rispondere in tempo reale alle esigenze aziendali.

L'integrazione con il cloud, per esempio, consente alle aziende di gestire i flussi di lavoro da qualsiasi luogo e in qualsiasi momento, migliorando l'efficienza operativa e riducendo la necessità di infrastrutture fisiche locali. La stampa connessa al cloud permette anche l'analisi dei dati in tempo reale, offrendo insights preziosi per otti-

mizzare l'uso delle risorse e ridurre gli sprechi.
L'adozione dell'IoT, d'altro canto, sta portando alla creazione di ecosistemi di stampa intelligenti, dove i dispositivi comunicano tra loro e con i sistemi aziendali per automatizzare i processi e prevenire problemi tecnici prima che si verifichino. Le stampanti dotate di sensori IoT possono monitorare continuamente lo stato delle componenti, prevedere quando è necessario un intervento di manutenzione e ordinare automaticamente i materiali di consumo.
Infine, l'intelligenza artificiale sta rivoluzionando la gestione della stampa con soluzioni che apprendono dalle abitudini degli utenti, ottimizzando i processi e riducendo al minimo l'intervento umano. In ambienti enterprise l'AI, combinata con l'analisi dei big data, può consentire di prevedere i trend di stampa e di adattare le risorse in modo più efficiente.

Impatto sul business e vantaggi della stampa connessa

L'evoluzione della stampa connessa non è solo una questione di innovazione tecnologica, ma di **risponde anche a specifiche esigenze di trasformazione digitale e revisione dei processi aziendali.** In un contesto in cui le aziende stanno cercando di digitalizzare i loro flussi lavoro per aumentare l'efficienza e ridurre i costi, la stampa connessa rappresenta, quindi, una soluzione che assume valenza strategica.

Una delle principali aree in cui la stampa connessa sta facendo la differenza è la gestione dei documenti. Le soluzioni di gestione documentale basate su cloud permettono alle aziende di digitalizzare e archiviare i documenti in modo sicuro, migliorando l'accesso e la condivisione delle informazioni. Questo è particolarmente importante in settori come quello legale, finanziario e sanitario, dove la gestione dei documenti è cruciale per il rispetto delle normative e la protezione dei dati sensibili.
Un aspetto cruciale della stampa connessa è la sua **capacità di supportare la gestione documentale** in un ambiente digitale. Ciò significa che i documenti possono essere scansionati, archiviati, condivisi e stampati direttamente dal cloud, facilitando l'accesso e la collaborazione a livello aziendale. Questo approccio riduce la necessità di copie cartacee e consente una gestione più sicura e tracciabile delle informazioni sensibili.
Inoltre, la stampa connessa offre la possibilità di implementare processi di stampa più sostenibili, riducendo l'uso di carta e inchiostro attraverso una gestione più efficiente delle risorse. Le aziende possono impostare politiche di stampa basate su regole che riducono gli sprechi limitando le stampe non necessarie, monitorando in tempo reale l'uso delle risorse e ottimizzando l'uso di carta e inchiostro.

Esempi e applicazioni settoriali

Diversi settori stanno già beneficiando delle tecnologie di stampa connessa. Nel settore sanitario, per esempio, la stampa connessa permette una gestione più efficiente dei dati dei pazienti, integrando i documenti cartacei con le cartelle cliniche elettroniche (EMR), migliorando la precisione e la rapidità di accesso alle informazioni critiche.

Nel settore **manifatturiero**, l'adozione di soluzioni di stampa connessa consente di gestire in modo centralizzato le diverse linee di produzione, migliorando la tracciabilità e riducendo i tempi di fermo macchina. Le stampanti intelligenti possono comunicare direttamente con i sistemi ERP aziendali, automatizzando il riordino delle parti di ricambio e garantendo che la produzione continui senza interruzioni.

Anche nel settore dell'**istruzione**, la stampa connessa sta avendo un impatto significativo, permettendo alle istituzioni educative di gestire in modo più efficace le risorse e ridurre i costi operativi. Gli studenti e il personale possono accedere ai servizi di stampa da qualsiasi dispositivo connesso alla rete, riducendo la necessità di hardware dedicato e semplificando la gestione dei documenti.

GLI APPROFONDIMENTI DI BIZZIT

L'impatto della stampa 4.0 sulla trasformazione digitale

continua a leggere

Prospettive future e trend evolutivi

Guardando al futuro, il mercato della stampa connessa continuerà a evolversi, spinto da nuove innovazioni e dall'aumento della domanda di soluzioni di stampa più efficienti e integrate. Tra i trend emergenti nei prossimi cinque anni, possiamo aspettarci una maggiore integrazione con l'AI e il machine learning, che permetteranno alle soluzioni di stampa di diventare sempre più autonome e **capaci di auto-ottimizzarsi**.

Inoltre, l'evoluzione delle reti 5G aprirà nuove possibilità per la stampa connessa, permettendo una comunicazione ancora più rapida ed efficiente tra i dispositivi e i sistemi aziendali. Questo avrà un impatto particolarmente rilevante nei settori ad alta intensità di dati, come quello sanitario e finanziario.

Infine, la sostenibilità rimarrà un tema centrale, con un aumento della domanda di soluzioni di stampa ecocompatibili e l'adozione di politiche aziendali che favoriscano la riduzione degli sprechi. Le aziende dovranno continuare a investire in tecnologie che permettano di monitorare e ridurre l'impatto ambientale delle loro operazioni di stampa.

STAMPA CONNESSA E SICUREZZA

La stampa connessa introduce anche nuove sfide in termini di sicurezza dei dati. Con dispositivi sempre più integrati nelle reti aziendali e connessi al cloud, il rischio di cyberattacchi e di violazioni della privacy aumenta considerevolmente. Per questo motivo, garantire la sicurezza della stampa connessa non è solo una necessità, ma un imperativo strategico per ogni azienda.
Le moderne soluzioni di stampa sicura si basano su una combinazione di tecnologie avanzate e best practice per proteggere i dati lungo tutto il ciclo di vita della stampa.
Una delle misure più efficaci è l'adozione della crittografia end-to-end, che protegge i dati sia durante la trasmissione che quando sono in fase di memorizzazione temporanea sui dispositivi. Questo garantisce che i documenti non possano essere intercettati o manipolati da terze parti non autorizzate.
Un altro elemento chiave è l'autenticazione multi-fattore (MFA), che aggiunge un ulteriore livello di sicurezza, richiedendo agli utenti di verificare la propria identità attraverso più metodi, come una password e un codice generato da una App di autenticazione. Questo riduce significativamente il rischio di accesso non autorizzato ai dispositivi di stampa.
Le stampanti connesse di ultima generazione sono inoltre dotate di funzioni di controllo degli accessi basate su ruoli, che consentono di configurare permessi specifici per diversi gruppi di utenti. In questo modo, solo il personale autorizzato può accedere a determinate funzionalità o stampare documenti sensibili.
Una tecnologia particolarmente utile per garantire la sicurezza dei documenti è la stampa sicura. Questa funzione trattiene i lavori di stampa in una coda sicura fino a quando l'utente non si autentica fisicamente presso il dispositivo, magari utilizzando una smart card o un badge aziendale. Ciò elimina il rischio che documenti riservati siano lasciati incustoditi nel vassoio della stampante, accessibili a chiunque.
Per proteggere ulteriormente le infrastrutture di stampa, le aziende possono implementare soluzioni di monitoraggio continuo che analizzano i log delle stampanti per rilevare comportamenti anomali o tentativi di accesso non autorizzato. Alcuni sistemi avanzati integrano l'intelligenza artificiale per identificare e rispondere in modo proattivo alle minacce, attivando "alert" in tempo reale o bloccando automaticamente le operazioni sospette.
Infine, è fondamentale che le aziende mantengano aggiornati i firmware e i software delle stampanti per proteggerli dalle vulnerabilità emergenti. Le patch di sicurezza devono essere applicate tempestivamente, e le reti su cui operano i dispositivi di stampa devono essere segmentate e protette da firewall e sistemi di prevenzione delle intrusioni.

Market review

I PRODUTTORI

PARTNERS
INFORMAZIONE E FORMAZIONE PER IL CANALE A VALORE

HP
Via Carlo Donat Cattin, 5
20063 Cernusco sul Naviglio (MI)

+39 02 3859 0383
www.hp.com

PUNTI DI FORZA

HP è rinomata per la tecnologia “HP Sure Start”, che protegge il BIOS delle stampanti da attacchi e manomissioni e per le soluzioni di stampa sicura con autenticazione multi-fattore e crittografia avanzata.

Hewlett-Packard

Strategia

HP adotta una strategia focalizzata sull’innovazione continua nel settore della stampa, integrando hardware, software e servizi cloud per migliorare produttività, sicurezza e sostenibilità. L’azienda punta a fornire soluzioni all’avanguardia che si adattano alle esigenze di aziende di tutte le dimensioni, promuovendo la stampa sicura e la gestione documentale centralizzata.

Offerta

HP offre una gamma completa di stampanti e multifunzione, inclusa la serie HP PageWide e il servizio HP Instant Ink, che automatizza la fornitura di inchiostro basata sull’uso effettivo. Le soluzioni HP si distinguono per l’integrazione con HP Security Manager e le capacità di stampa gestita (MPS), che ottimizzano i costi e migliorano l’efficienza operativa.

XEROX CORPORATION
Via Nazionale 9
20121 Milano

+39 02 507 261
www.xerox.it

PUNTI DI FORZA

Xerox si distingue per la sua capacità di integrare soluzioni di stampa connesse con tecnologie come l’intelligenza artificiale e l’analisi dei dati, con sicurezza integrata e monitoraggio delle minacce in tempo reale.

Xerox Corporation

Strategia

Xerox si concentra sull’innovazione nella stampa e gestione documentale, con soluzioni che automatizzano i processi aziendali e migliorano la collaborazione, puntando sulla trasformazione digitale.

Offerta

Xerox offre una gamma completa di stampanti multifunzione (MFP), stampanti di produzione e soluzioni di gestione documentale. La piattaforma Xerox ConnectKey trasforma i dispositivi in hub digitali, consentendo l’integrazione con app di terze parti e la creazione di flussi di lavoro personalizzati.

CANON
Via Milano 8
20097 San Donato Milanese (MI)

+39 02 02 8248 1
www.canon.it

PUNTI DI FORZA
Canon è apprezzata per la qualità di stampa e per la tecnologia Canon ULM (Unified Login Manager), che offre gestione avanzata degli accessi utente, garantendo che solo il personale autorizzato possa accedere ai documenti stampati.

Canon

Strategia
Canon adotta una strategia incentrata sull'innovazione tecnologica e sulla qualità del prodotto, offrendo soluzioni di stampa che soddisfano le esigenze di aziende di ogni dimensione. L'azienda è particolarmente attenta alla sostenibilità, sviluppando tecnologie che riducono l'impatto ambientale.

Offerta
Canon offre una vasta gamma di stampanti, inclusi modelli laser, a getto d'inchiostro e multifunzione. La serie Canon ImageRunner Advance è particolarmente apprezzata per la sua integrazione con software di gestione documentale e sistemi di sicurezza aziendale.

RICOH
Viale G. Matteotti, 62
20092 Cinisello Balsamo (MI)

+39 02 618 201
www.ricoh.it

PUNTI DI FORZA
Ricoh è nota anche per l'adozione di tecnologie eco-sostenibili e per la riduzione delle emissioni di CO2. Le sue soluzioni includono anche funzionalità di sicurezza avanzate, come l'autenticazione utente tramite badge e il monitoraggio delle attività di stampa in tempo reale.

Ricoh

Strategia
Ricoh si concentra sulla trasformazione digitale, offrendo soluzioni di stampa e gestione documentale che si integrano perfettamente con le infrastrutture IT aziendali esistenti. L'azienda punta a migliorare l'efficienza operativa delle imprese attraverso l'innovazione tecnologica e servizi di consulenza avanzata.

Offerta
Ricoh offre una vasta gamma di dispositivi multifunzione, stampanti, soluzioni di gestione documentale e software per l'automazione dei flussi di lavoro. Le soluzioni Ricoh Smart Integration permettono di connettere i dispositivi alle piattaforme cloud e di gestire i documenti in modo sicuro ed efficiente.

KONICA MINOLTA
Via Stephenson, 37
20157 Milano

+39 02 390 121
www.konicaminolta.it

PUNTI DI FORZA
Konica Minolta si distingue per la piattaforma Workplace Hub, una soluzione all-in-one che combina stampa, gestione IT e comunicazione. Le sue soluzioni sono altamente scalabili e adatte sia per piccole imprese che per grandi organizzazioni.

Konica Minolta

Strategia
Konica Minolta adotta una strategia di digitalizzazione e automazione, offrendo soluzioni che supportano la trasformazione digitale delle imprese. L'azienda si concentra su soluzioni end-to-end che integrano stampa, gestione documentale e IT, aiutando le aziende a migliorare la produttività e a ridurre i costi.

Offerta
Konica Minolta offre una vasta gamma di stampanti multifunzione, soluzioni di stampa sicura e software per la gestione documentale. La serie Bizhub di Konica Minolta è conosciuta per la sua capacità di integrarsi con le infrastrutture IT aziendali e di supportare flussi di lavoro digitali.

EPSON
Via M. Vigiani, 73
20156 Milano

+39 02 66 306 306
www.epson.it

PUNTI DI FORZA
Epson è leader nella tecnologia di stampa a getto d'inchiostro con PrecisionCore, che offre alta velocità e qualità senza compromessi. Le sue soluzioni includono anche funzionalità di stampa remota e sicura, con possibilità di stampa diretta da dispositivi mobili.vità di stampa in tempo reale.

Epson

Strategia
Epson si distingue per il suo impegno verso la sostenibilità e l'innovazione tecnologica. L'azienda si concentra sulla produzione di soluzioni di stampa che offrono alta qualità e basso impatto ambientale, con un occhio di riguardo per l'efficienza energetica e la riduzione dei costi operativi.

Offerta
Epson offre una vasta gamma di stampanti a getto d'inchiostro, stampanti laser e soluzioni multifunzione. La linea di stampanti EcoTank di Epson, che utilizza serbatoi di inchiostro ricaricabili, è particolarmente apprezzata per la sua convenienza e per la riduzione dei rifiuti.

BROTHER
Via Sant'Antonio, 15
20023 Cerro Maggiore (MI)

+39 0331 501 020
www.brother.it

PUNTI DI FORZA
Brother si distingue per la facilità di installazione e la manutenzione ridotta, ideale per piccole e medie imprese. Le soluzioni Brother includono funzionalità di stampa mobile e gestione centralizzata delle operazioni tramite app dedicata.

Brother

Strategia
Brother adotta una strategia orientata alla versatilità e alla facilità d'uso, offrendo soluzioni di stampa affidabili e convenienti, ideali per piccole e medie imprese. L'azienda è nota per l'attenzione alla qualità e alla durata dei suoi prodotti.

Offerta
Brother offre una gamma completa di stampanti laser, multifunzione e a getto d'inchiostro, insieme a soluzioni per la stampa mobile e la gestione documentale. Le stampanti della serie Brother HL-L sono conosciute per l'efficienza energetica e la capacità di gestire elevati volumi di stampa con costi operativi contenuti.

LEXMARK
Viale Sarca, 222
20126 Milano

+39 02 64 11 31
www.lexmark.it

PUNTI DI FORZA
Lexmark si distingue anche per le sue soluzioni di sicurezza avanzate, che includono il Lexmark Secure Print Release, una funzione che trattiene i lavori di stampa fino a quando l'utente non si autentica fisicamente presso il dispositivo.

Lexmark

Strategia
Lexmark è focalizzata sull'offerta di soluzioni di stampa intelligenti che supportano la gestione avanzata dei documenti e la sicurezza dei dati. L'azienda si distingue per l'attenzione alla qualità e all'innovazione, con soluzioni progettate per rispondere alle esigenze delle grandi imprese. Lexmark, che adotta una strategia incentrata sull'innovazione tecnologica e sulla sostenibilità, è fortemente impegnata nella digitalizzazione dei processi aziendali, integrando le sue stampanti e multifunzione con avanzati servizi cloud e soluzioni di gestione documentale.

Offerta
Lexmark offre una gamma di stampanti laser e multifunzione, con soluzioni avanzate di gestione documentale e integrazione con servizi cloud. Le stampanti Lexmark della serie CX sono particolarmente apprezzate per la loro velocità di stampa e per la qualità delle immagini, ideali per uffici ad alto volume.

KYOCERA Document Solutions
Viale Milano, 3
20097 San Donato Milanese (MI)

+39 02 514 235
kyoceradocumentsolutions.it

PUNTI DI FORZA
Kyocera è rinomata per l'uso di componenti a lunga durata nei suoi dispositivi, che riducono la necessità di manutenzione e l'impatto ambientale. Le soluzioni Kyocera includono anche funzionalità di gestione centralizzata, per monitorare e controllare le operazioni di stampa da un'unica piattaforma.

Kyocera Document Solutions

Strategia
Kyocera si concentra sull'offerta di soluzioni di stampa sostenibili e ad alta efficienza, con un forte impegno verso l'innovazione e la riduzione dell'impatto ambientale. L'azienda promuove l'adozione di soluzioni che aiutano le imprese a ottimizzare i loro processi documentali e a ridurre i costi operativi.

Offerta
Kyocera offre una gamma di stampanti multifunzione, stampanti laser e soluzioni di gestione documentale. Le stampanti della serie TaskAlfa sono conosciute per la loro durata e affidabilità, ideali per ambienti di lavoro esigenti

SHARP
Via Stephenson, 37/A
20157 Milano

+39 02 39 05 21
www.sharp.it

PUNTI DI FORZA
Sharp si distingue per l'integrazione delle sue soluzioni di stampa con la piattaforma Sharp OSA (Open Systems Architecture), che consente alle stampanti di comunicare con altre applicazioni aziendali e di automatizzare i flussi di lavoro.

Sharp

Strategia
Sharp si concentra sull'offerta di soluzioni di stampa connesse che combinano funzionalità avanzate con un'eccezionale facilità d'uso. L'azienda punta a migliorare la produttività aziendale attraverso l'integrazione delle sue stampanti con le infrastrutture IT e i servizi cloud.

Offerta
Sharp offre una vasta gamma di stampanti multifunzione, progettate per soddisfare le esigenze di piccole e medie imprese, così come grandi organizzazioni. Le stampanti della serie MX sono apprezzate per la loro capacità di gestione dei documenti e per le funzionalità di sicurezza integrate.

bizIT.it

MAGAZINE ONLINE DI ICT E TECNOLOGIA

INFORMATION COMMUNICATION TECHNOLOGY

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

Continua a seguirci su:
https://bizzit.it/